UNIVERSIDAD DE COSTA RICA

FACULTAD DE DERECHO

TESIS DE GRADO PARA OPTAR POR EL TÍTULO DE LICENCIATURA EN DERECHO

“Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos”

Autora

Daniela Salas Peña

Abril, 2010

San José, Sede Rodrigo Facio

8 de abril de 2010
FD-AI-T- 423-10

Doctor
Daniel Gadea Nieto
Decano
Facultad de Derecho

Estimado Decano:

Para los efectos reglamentarios correspondientes, le informo que el Trabajo Final de Graduación (categoría Tesis) del (de la) estudiante **DANIELA SALAS PEÑA**, Carné **A34783** titulado:

"RESPONSABILIDAD CIVIL BANCARIA FRENTE AL CLIENTE POR DELITOS INFORMÁTICOS".

La tesis anterior, fue aprobado por el Comité Asesor, para que sea sometido a su defensa final. Asimismo, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo apruebo en el mismo sentido.

En el mismo orden de ideas, le presento a los (as) miembros (as) del Tribunal Examinador de la presente Tesis, a quienes en la fecha abajo indicada, se les entregó ejemplar de Trabajo Final de Graduación.

Tribunal Examinador	
Presidente (a)	Prof. Carlos Estradas Navas
Secretario (a)	Prof. Adriana Rojas Rivero
Informante	Prof. Víctor Pérez Vargas
Miembro (a)	Prof. Andrés Montejo Morales
Miembro (a)	Prof. Federico Torrealba Navas

Por último le informo que la réplica o defensa de la tesis, será el día 26 de abril de 2010, a las 6:00 p.m., en la Sala de Tesis ubicada en el quinto de la Facultad de Derecho.

Atentamente,

FACULTAD DE DERECHO
UNIVERSIDAD DE COSTA RICA
LUCEN ASPICIO
AREA DE INVESTIGACION

Dr. Olivier Rémy Gassiot
DIRECTOR

San José, 6 de febrero del 2010

Dr. Olivier Rémy Gassiot
Director del Área de Investigación
Facultad de Derecho
U.C.R.
Pte.

Estimado Señor:

Tengo el gusto de comunicarle que he terminado la revisión del trabajo final de graduación de **Daniela Salas Peña**, titulado **"Responsabilidad Civil Bancaria frente al Cliente por Delitos Informáticos".**

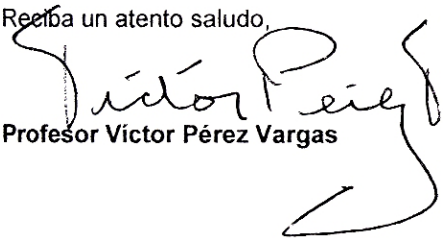
La autora inicia el desarrollo del tema con algunas generalidades sobre la Responsabilidad Civil (contractual y extracontractual) y los criterios de imputación (subjetiva y objetiva). Seguidamente, explica ampliamente los caracteres del fraude informático, las diversas modalidades como éste opera y la responsabilidad que de él deriva para los bancos.

Es en relación con el criterio de imputación objetivo antes mencionado que la jurisprudencia ha realizado interesantes desarrollos (con base en la Ley de Libre Competencia y Defensa Efectiva del Consumidor), los cuales analiza exhaustivamente la autora, todos ellos centrados en el conflicto entre los consumidores y los bancos, como resultado de un delito informático desarrollado en la Banca por Internet. También nos da cuenta de las medidas de seguridad que han sido desarrolladas y la que han sido tomadas en cuenta a la fecha por las entidades bancarias que operan en Costa Rica.

Daniela logra demostrar su hipótesis en el sentido de que las entidades bancarias, al ofrecer un servicio y obtener un beneficio por él, deben responder, tal y como lo indica la Ley, por todos aquellos daños que como resultado de esta actividad se produzcan. Así, la responsabilidad civil que existe es objetiva, y por lo tanto, los bancos son responsables de todos aquellos perjuicios que por su la prestación del servicio se hayan ocasionado. De demostrarse alguna causa extraña, se exime al banco de la responsabilidad que le genera un delito informático sufrido por sus clientes.

La exposición es muy completa, está muy bien sistematizada, constituye un valioso aporte y cumple a cabalidad el objetivo general: "examinar la existencia de responsabilidad civil de una entidad bancaria cuando alguno de sus clientes es víctima de un delito informático". Por las razones expuestas y por cumplir los requisitos correspondientes, es un gusto para mí otorgarle la aprobación, sin reservas, para que pueda pasar a su etapa de réplica.

Reciba un atento saludo,



Profesor Víctor Pérez Vargas

Ciudad Universitaria "Rodrigo Facio", 8 de abril de 2010.

Sr. Dr. Olivier Remy Gassiot
Director
AREA DE INVESTIGACION
Facultad de Derecho
Universidad de Costa Rica.

Estimado señor Director:

En mi condición de Lector del trabajo final de graduación de la egresada DANIELA SALAS PEÑA carnet A34783 titulado *RESPONSABILIDAD CIVIL BANCARIA FRENTE AL CLIENTE POR DELITOS INFORMATICOS* me es grato comunicarle por la presente que le he impartido mi aprobación para que sea discutida en réplica ante el Tribunal Examinador respectivo, por cuanto de la revisión que de su investigación he hecho estimo que cumple a cabalidad los requisitos de forma y fondo requeridos a este efecto.

Sin otro particular que expresarle las muestras de mi consideración y estima, me suscribo,

Atentamente,

Prof. Carlos Manuel Estrada Navas
LECTOR

CMEN/msc
c.c. arch

MONTEJO
ASSOCIATES

San José, 06 de abril, 2010

Doctor
Olivier Rémy Gassiot
Director Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Presente

Estimado señor:

En mi condición de lector de la tesis titulada **"Responsabilidad Civil Bancaria frente al cliente por delitos informáticos."**, de la estudiante **Daniela Salas Peña**, carné A34783; con sumo placer manifiesto lo siguiente:

He dado lectura detallada al trabajo final de graduación de la señorita Salas Peña, la cual cumple con todos los requisitos de forma y fondo establecidos en la normativa universitaria, por lo que procedo a aprobarla para ser presentada al Tribunal de Graduación correspondiente.

De usted con todo respeto,

Lic. Andrés Montejo Morales, LL.M.
Lector

Lic. Andrés Montejo Morales
ABOGADO
Carné
No. 4580
San José, C.R.

je

Dedicatoria

A Dios Padre Celestial,

Por acompañarme en cada paso, en quien TODO lo puedo, en quien deposito mi confianza.

A mis padres y hermana,

Arquitectos de mi vida y felicidad, agradezco inmensamente a Dios haberlos escogido como mi familia, su amor, esfuerzo y confianza han permitido que alcancemos este nuestro triunfo. Los amo.

A Tita,

Mujer maravillosa y ejemplar, hoy tu fortaleza, bondad, tenacidad y entrega dan un fruto más. Tu valentía es mi ejemplo, tu sonrisa mi luz.

A Javi,

Mi fuente inagotable de amor y esperanza.

Te dedico con todo mi amor este proyecto, tan tuyo como mío, en el que confiaste minuto a minuto. Sin tu ayuda sin límites no habría logrado finalizar este sueño, sin tus palabras de ánimo y tu eterno amor. Gracias por darme alas y volar junto a mí.

"Yo te amo para comenzar a amarte,

para recomenzar el infinito

y para no dejar de amarte nunca…" P.N.

Agradecimientos

A mi excelente director Dr. Víctor Pérez Vargas, por sus acertados consejos, su característica amabilidad y su disposición a colaborar en este proyecto en todo momento, mi eterna gratitud, es un honor para mí contar con su dirección. También agradezco a quienes aceptaron el reto de formar parte de esta investigación desde el inicio, el Lic. Carlos Estrada Navas y el Lic. Andrés Montejo, muchas gracias por ser impecables lectores. A la Licda. Adriana Rojas Rivero y al Lic. Federico Torrealba, por su valioso aporte e inclusión en el Tribunal Examinador. Al Dr. Gastón Certad Maroto (q.d.D.g.) quien me ofreció su destacada participación en la Tesis, por su ejemplo de vida.

A mi familia en general, mis queridos tíos, primos y a Gil, gracias infinitas por su apoyo incondicional, por sus palabras de ánimo, oraciones y por su interés permanente en todo el desarrollo de mi vida. Este proyecto es también suyo. Los quiero mucho, son un regalo de Dios.

A la familia Espinoza Rivero, mi segunda familia, son una bendición para mí, les agradezco igualmente el apoyo y la confianza que siempre me han dado, son parte esencial en mi vida.

A mis amigos, la familia que escogemos, sus palabras, demostraciones de cariño y presencia en mi vida son imprescindibles. No tengo palabras para agradecer la paciencia y la fe que siempre me han tenido.

A todos los profesionales que colaboraron amablemente en esta investigación, gracias por brindarme su valioso aporte.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE ABREVIATURAS

ACL

Asociación de Consumidores Libres

Ley de Defensa al Consumidor

Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (Ley 7472)

Sala Primera

Sala Primera de la Corte Suprema de Justicia

Sala Tercera

Sala Tercera de la Corte Suprema de Justicia

Tribunal Contencioso

Tribunal Procesal Contencioso Administrativo y Civil de Hacienda

La Guía

Guía para la Incorporación de la Ley Modelo de la CNUMDI sobre Comercio Electrónico

Resumen

Salas Peña Daniela (2010). Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos.

La presente investigación trata el tema de la Responsabilidad Civil Bancaria frente al cliente por delitos informáticos. Para ello, se tiene como objetivo general el examinar la existencia de responsabilidad civil de una entidad bancaria cuando alguno de sus clientes es víctima de un delito informático. Con el fin de realizar este objetivo, así como los específicos, se recurre a fuentes primarias que han tratado los temas que conjugan esta investigación, entre ellos, la Responsabilidad Civil, la imputación objetiva, los delitos informáticos, mecanismos de seguridad, derecho del consumidor, entre otros. Además, se recurre a la investigación de campo, para que a través de las entrevistas y encuestas se obtenga de primera mano la información necesaria para el desarrollo de la investigación. La hipótesis que se maneja es que efectivamente los bancos tienen responsabilidad objetiva según la ley 7472 por todos aquellos daños que su actividad ocasione, siempre y cuando no se pruebe la existencia de un eximente de responsabilidad.

El derecho del consumidor se ha visto impulsado con reformas constitucionales, criterios jurisprudenciales y con la ley 7472, por ello los afectados por delitos informáticos en el servicio de Banca por Internet, basan su posición en la responsabilidad objetiva establecida en el artículo 35 de la ley citada. Por su parte, los Bancos consideran que no existe responsabilidad que se les pueda imputar pues se trata de un riesgo propio del servicio de Internet que no es ofrecido por ellos. La jurisprudencia, tanto del Tribunal Contencioso Administrativo como de la Sala Primera ha coincidido mayoritariamente en darles la razón a los consumidores y condenar a los bancos.

A raíz de este conflicto de novedosos alcances, es que se busca alcanzar una alternativa objetiva y crítica que sirva como opción para solucionar la incertidumbre que existe al respecto. Dentro de la tesis se desarrolla el tema de la Responsabilidad Civil, dividida en contractual y extracontractual, también se hace alusión a los tipos de imputación de la responsabilidad, sea la subjetiva que es el típico criterio de imputación, o la objetiva, que depende de varios elementos, entre ellos que se encuentre tipificada y que exista un riesgo creado. La jurisprudencia ha marcado la pauta en nuestro país, por lo que se analizan algunas sentencias consideradas interesantes para la investigación.

Posteriormente, se estudia con detalle el tema del Comercio Electrónico con sus correspondientes ramas, por ejemplo, la Banca por Internet. Bajo esta perspectiva, se pasa al estudio de lo que ha sido el mayor problema para el usuario de este tipo de tecnologías, los delitos informáticos. Así, una vez definidos los principales delitos que han perjudicado a los clientes, se indican las medidas de seguridad que han sido desarrolladas y la que han sido tomadas en cuenta a la fecha por las entidades bancarias que operan en Costa Rica.

Por último, enlazando la información dada en los capítulos precedentes, se arriba a las principales conclusiones del tema en cuestión. Se propone la capacitación y concientización como un mecanismo más de seguridad, que no ha sido tomado en cuenta según los resultados arrojados por las encuestas y del estudio de los casos presentados por fraudes informáticos. Además, se plantea la importancia de crear un Reglamento o disposición de la SUGEF o del CONASSIF que obligue a los bancos que van a brindar un servicio de Banca por Internet a sujetarse a una serie de reglas mínimas que establezcan la seguridad que deben de poseer.

Ficha bibliográfica

SALAS PEÑA, Daniela (2010). Responsabilidad Civil Bancaria frente al cliente por delitos informáticos. Tesis de Licenciatura en Derecho. Universidad de Costa Rica. San José, Costa Rica.

Director: Dr. Víctor Pérez Vargas.

Descriptores

Derecho Privado. Responsabilidad Civil. Responsabilidad Objetiva. Responsabilidad Bancaria. Banca Electrónica. Banca por Internet. Derecho Informático. Fraudes informáticos. Delitos Informáticos. Derecho del Consumidor. Procesos Colectivos. Mecanismos de Seguridad Informática. Firma Digital. Certificados Digitales.

Introducción

JUSTIFICACIÓN

A finales del siglo pasado y en el desarrollo del presente, la tecnología ha avanzado a pasos agigantados, poniendo al alcance de los seres humanos una serie de herramientas con las que quizá ni siquiera se soñaba en la antigüedad. El avance de la ciencia y la técnica han facilitado las labores diarias de una humanidad globalizada y moderna, pero también se han convertido en un instrumento del que se valen muchos para cometer acciones contrarias a los fines para los que dichas novedades han sido creadas y así sacar provecho ilegítimo de ello.

Las transacciones bancarias realizadas a través de Internet, por medio de la Banca por Internet, se han convertido en un método muy aplicado y con gran aceptación social. La efectividad y facilidad que aporta esta moderna herramienta, ha logrado el convencimiento y la aprobación de millones de personas que alrededor del mundo, y Costa Rica no es la excepción, quienes hoy realizan movimientos miles de esta manera. La comodidad y el ahorro de tiempo se perfilan como algunos de los mayores beneficios que aporta este sistema, pues no es necesario acudir a una sucursal del Banco para realizar

diversas transacciones dinerarias, ya que se puede acceder desde cualquier parte del mundo mediante Internet.

Sin embargo, a pesar de las bondades que brinda este avanzado instrumento, no ha quedado intacto a las vulneraciones generadas por personas inescrupulosas que buscan su beneficio patrimonial de forma ilícita. Diversas estrategias han sido utilizadas para cumplir con este cometido, por ejemplo, a través del engaño y la manipulación de los usuarios para que éstos les brinden a los "crackers" sus elementos de legitimación o datos personales, tales como su clave de acceso (PIN) y su identificación y de esta manera atacar a lo que se considera el "eslabón débil".

Al respecto de este tipo de situaciones y las consecuencias que producen, se han desarrollado una serie de controversias que versan sobre la responsabilidad que puede o no tener una entidad bancaria, cuando brinda el servicio de Banca por Internet y sus clientes se han visto afectados por el delitos informáticos.

La posición de los usuarios se fundamenta en la existencia de una Responsabilidad Objetiva por parte de los Bancos, pues el servicio que se presta es considerado riesgoso y además no se han tomado las medidas de seguridad necesarias y suficientes, por lo tanto deben responder por los daños que con esta actividad se puedan producir.

Por otro lado, la posición de los bancos es que no debe aplicar la Responsabilidad por riesgo cuando el hecho dañoso ha sido creado por un tercero y por lo tanto no puede achacarse la responsabilidad al banco, además, se alega la existencia de una relación contractual entre las partes y las disposiciones que ahí se aceptaron por los clientes son vinculantes entre las partes. Se ha dicho que el banco no puede controlar las actuaciones negligentes de la víctima en tanto exista un mal manejo de su información, fue imprudente cuando accedió a las páginas electrónicas del Banco, brindó contraseñas y datos confidenciales a terceros y demás posibilidades.

En esta encrucijada se encontraron los Tribunales de Costa Rica, que tramitan una elevada cantidad de casos de personas en estas circunstancias, y que han emitido los primeros criterios al respecto, acogiendo la tesis de los clientes. El criterio ha sido confirmado incluso por la Sala Primera.

Como es normal, los problemas sociales se desarrollan a mayor velocidad que la respuesta legal para resolverlos, y máxime en temas de tecnología, en donde la constante es el cambio y éste se produce a cada segundo. Es así, como se debe intentar hallar una solución justa y clara sobre los asuntos que tanta polémica generan.

Con esta investigación se pretende, brindar un criterio sobre la resolución de dicho conflicto, analizando de forma integral las distintas aristas que forman parte del problema, de esta manera se busca explicar esta compleja situación tanto en el ámbito jurídico como en el informático, con el fin de obtener una respuesta objetiva, equitativa e informada al respecto, pero sobre todo dotando de mecanismos que permitan disminuir el número de víctimas y solventar las deficiencias existentes en protección de los intereses de la sociedad. Para tales efectos, se revisará la doctrina y legislación existente, los delitos informáticos y las medidas de seguridad empleadas, así como las posiciones de los sectores en juego y las soluciones que se han generado en la sede judicial

El tema propuesto reviste de elevada relevancia en la sociedad actual, pues se encuentran en disputa una serie de intereses que el Estado debe tutelar y así funcionar como respuesta adecuada y actual para sus ciudadanos.

OBJETIVOS

OBJETIVO GENERAL:

Examinar la existencia de responsabilidad civil de una entidad bancaria cuando alguno de sus clientes es víctima de un delito informático.

OBJETIVOS ESPECÍFICOS:

- Estudiar los tipos de Responsabilidad Civil que se aplican en el Sistema Jurídico costarricense y los criterios de imputación de responsabilidad.

- Realizar un análisis de la jurisprudencia existente sobre la responsabilidad civil objetiva, con atención a los criterios esgrimidos al respecto por distintos órganos jurisdiccionales.

- Analizar la creciente utilización del servicio de Banca por Internet de cara al veloz surgimiento de delitos informáticos, así como algunas de las medidas de seguridad

desarrolladas y las que son aplicadas por los Bancos para sus clientes como respuesta a esta problemática.

- Estudiar el surgimiento del Derecho del Consumidor y su aplicación dentro del derecho costarricense, así como el régimen de responsabilidad que establece la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

- Revisar las sentencias dictadas por el Tribunal Contencioso Administrativo y la Sala Primera de la Corte Suprema de Justicia en cuanto a la responsabilidad civil bancaria frente al cliente por delitos informáticos.

HIPÓTESIS

Las entidades bancarias, al ofrecer un servicio y obtener un beneficio por él, deben responder tal y como lo indica la Ley Promoción de la Competencia y Defensa Efectiva del Consumidor, por todos aquellos daños que como resultado de esta actividad se produzcan. Así, la responsabilidad civil que existe es objetiva, y por lo tanto, los bancos son responsables de todos aquellos perjuicios que por su conducta se hayan ocasionado. De demostrarse alguna de las eximentes de responsabilidad estipuladas en la ley mencionada, se exime al banco de la responsabilidad que le genera un delito informático sufrido por sus clientes.

MARCO TEÓRICO

I. LA RESPONSABILIDAD.

El término Responsabilidad tiene distintas acepciones, ya que es una palabra comúnmente utilizada para distintos fines. Incluso en el Derecho, esta palabra se utiliza tanto en la normativa como en el lenguaje jurídico con significados distintos. Para este trabajo resulta muy importante la siguiente definición de responsabilidad: "Situación por la cual se realiza la atribución de un efecto jurídico "de necesidad" (de un resarcimiento), sea como consecuencia de una culpabilidad o de un riesgo creado en las hipótesis de responsabilidad extracontractual o de la violación de un vínculo preexistente en los casos de responsabilidad contractual."[1]

Tal y como explica en Dr. Víctor Pérez Vargas en su libro Derecho Privado, no debe confundirse el concepto de Responsabilidad con el de obligación, pues esta última es el resultado de una situación jurídica que se le imputa a un sujeto, es la atribución de eficacia en que consiste la responsabilidad.

[1] PÉREZ VARGAS, Víctor (1994). *Derecho Privado*. San José, Costa Rica. Tercera Edición. Litografía e Imprenta LIL, S.A. P. 384.

Así, extrayendo ideas de distintos autores[2] se llega a la conclusión que responsabilidad es aquella situación jurídica en la que el patrimonio de una persona (física o jurídica) debe responder para resarcir por un daño producido, como resultado de este daño se genera una obligación, que es precisamente el resarcimiento. Se distingue dependiendo de la existencia de un contrato entre las partes o no, la responsabilidad civil contractual de la responsabilidad civil extracontractual.

II. RESPONSABILIDAD CIVIL DERIVADA DE UN HECHO PUNIBLE

A este tipo de Responsabilidad Civil también se le conoce como "ex delicto", teniendo como peculiaridad que el hecho que ocasiona el daño jurídicamente resarcible es punible, según el Derecho Penal. Por esta razón, no solamente se rige por el derecho civil, sino que encuentra de igual modo regulación dentro de otra rama del derecho, a saber el derecho penal.

Se debe recordar que el fundamento de la reparación civil es el daño, y en ocasiones este daño puede provenir de un hecho que se encuentra regulado dentro del ámbito penal como un delito. Así, la tutela jurídica para la víctima o sujeto pasivo se

[2] Además de la referencia mencionada supra, ver en igual sentido a MONTERO PIÑA, Fernando (1999). *Obligaciones*. San José, Costa Rica. Premiá Editores. P.313.

encuentra en dos sectores del ordenamiento jurídico, con distintas consecuencias para el sujeto activo.

En el sistema de responsabilidad civil lo importante es la existencia del daño, pues la base para el resarcimiento es justamente la producción de éste. El sistema penal funciona de manera distinta, ya que para que se considere la comisión de un delito debe demostrarse la existencia una acción típica, antijurídica y culpable. Sin embargo, si en el proceso penal no se determina la existencia de un delito pero sí la de un daño, puede condenarse civilmente al accionado, tal y como lo indica el siguiente extracto de una sentencia:

> *"(…)conforme al elenco de hechos demostrados para la resolución penal del asunto pero aplicables a los extremos civiles es posible determinar en un primer momento que se ha configurado una acción dañosa que aunque no resultó típica penalmente es generadora de responsabilidad civil directamente ocasionada por la publicación de un hecho falso desacreditante e injurioso en un medio escrito."*[3]

[3] Sala Tercera de la Corte Suprema de Justicia, Resolución número 2004-00535 de las 9:05 horas del 21 de mayo de 2004.

III. DELITOS INFORMÁTICOS.

Con el desarrollo de nuevas tecnologías y sobretodo con el incremento acelerado de la utilización del Internet como medio para realizar toda una serie de actividades económicas, se han producido de manera paralela los denominados delitos informáticos.

Los delitos informáticos pueden ser definidos como: "La acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas –hardware- o de los programas –software-"[4]

Con esta definición se hace referencia sólo a aquellos casos en los cuales se realiza un delito por medios informáticos y no a los delitos en los que se interviene, no de forma esencial, un elemento informático.[5]

[4] DÁVARA RODRÍGUEZ, Miguel Ángel. Citado por CHINCHILLA SANDÍ, Carlos (2004). *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. San José, Costa Rica. Ediciones Farben. P. 25

[5] CHINCHILLA SANDÍ, Carlos (2004). *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. San José, Costa Rica. Ediciones Farben. P. 25

Debe advertirse que brindar una única definición de delito informático resulta una labor sumamente complicada, pues posee múltiples concepciones y se le enlaza con otros elementos similares. Sin embargo, se entiende que la palabra delito informático es la más general y la que abarca otro tipo de expresiones similares para denominar este tipo de delincuencia.

Para la comisión de un delito informático se tiene como requisito indispensable la utilización de un equipo de cómputo (computadora) y la tecnología del mismo. Se encuentran, además, dos sujetos dentro del campo de acción de los delitos informáticos: un sujeto activo y un sujeto pasivo. Los primeros generalmente poseen importantes conocimientos en el campo de la informática y logran tener acceso por distintas vías de la información confidencial de otras personas.

Existen, por ejemplo, aquellos sujetos que por su trabajo cuentan con un acceso directo a los datos privados de una persona, por ejemplo, un empleado de una institución financiera; quien por su posición ocupacional posee acceso a un sistema y se sirve de ello para cometer un ilícito, incurre en lo que se ha llamado delito ocupacional.

El sujeto pasivo es aquella persona o entidad en la que recae la conducta del sujeto activo. Es quien sufre un daño provocado por el sujeto activo, por ejemplo, un

Banco al que se le vulneran sus sistemas informáticos para acceder a las cuentas de sus clientes.

Este tipo de ilícito puede clasificarse a partir de dos criterios iniciales, a saber, si es utilizado como instrumento o medio o como fin u objetivo.[6] Además, tienen como características la rapidez en el tiempo, la posición cercana al perjudicado y la facilidad de encubrir el hecho delictivo.[7]

Para el Dr. Carlos Chinchilla Sandí existen una serie de conductas que se consideran delitos informáticos, se hace notar que se trata de una clasificación *numerus apertus* y entre ellas se encuentran: manipulación en el ingreso de los datos (insiders) que es un verdadero fraude informático, conocido como sustracción de datos, es el delito informático más común. Otro caso es el de Manipulación en el procesamiento de datos ingresados, por medio del cual el autor manipula los datos que contiene la computadora, es decir, procesa dicha información. Es común que se utilice en método denominado "caballo de Troya", que consiste en insertar instrucciones de forma encubierta en un

[6] TÉLLEZ VALDÉZ. Citado por CHINCHILLA SANDÍ, Carlos (2004). *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. San José, Costa Rica. Primera edición. Ediciones Farben. P. 28

[7] CHINCHILLA SANDÍ, Carlos. op. cit. P.37

programa informático para que, dentro de su funcionamiento normal, pueda realizar una tarea no autorizada.[8]

Se señalan también como delitos informáticos: la Manipulación en los datos de salida (*outsiders*), la manipulación de programas ("Técnica del Salami"), intromisión en las bases de datos, la estafa informática (el autor altera o manipula -engaña- el ingreso, procesamiento y salida de datos de un sistema de cómputo por medio del empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema, del cual se pueda generar un perjuicio a un tercero), fraudes contra sistemas (daños o modificaciones de programas o datos computarizados), falsificaciones informáticas, entre otros.[9]

La Sala Tercera de la Corte Suprema de Justicia define en su voto 148-2006 de las nueve horas del veinticuatro de febrero del dos mil seis el delito informático:

> *"En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). "Por*

[8] Ibidem. PP. 39-60.
[9] CHINCHILLA SANDÍ, C. op. cit. PP. 39-60.

una parte, el National Center for Computer Crime Data indica que "el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes". De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el "delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos". Asimismo, William Cashion – estadounidense experto en informática – señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología" (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o

resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema."[10]

DELIMITACIONES CONCEPTUALES

Consumidor.

Toda persona física o entidad de hecho o de derecho, que, como destinatario final, adquiere, disfruta o utiliza los bienes o los servicios, o bien, recibe información o propuestas para ello. También se considera consumidor al pequeño industrial o al artesano - en los términos definidos en el Reglamento de esta ley - que adquiera productos terminados o insumos para integrarlos en los procesos para producir, transformar, comercializar o prestar servicios a terceros.[11]

[10] Sala Tercera de la Corte Suprema de Justicia. Sentencia 148-2006 de las nueve horas del veinticuatro de febrero del dos mil seis

[11] Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, N° 7472 de 20 de diciembre de 1994, art. 2

Cuenta cliente.

Estructura estandarizada del número de cuenta utilizado por las entidades participantes para identificar las distintas líneas de negocio (cuentas corrientes, cuentas de ahorros o cualquier otra cuenta de fondos a la vista o de dinero electrónico, tarjetas de crédito y cualquier otro producto financiero) de los clientes de las entidades financieras, utilizadas por éstos para realizar transacciones interbancarias. Esta cuenta constituye el domicilio financiero del cliente.[12]

ESTRUCTURA

La presente investigación consta de tres capítulos. En el primero de ellos se analizan los tipos de Responsabilidad que existen, los criterios de imputación aplicables y la jurisprudencia que se ha desarrollado con base en el tema de Responsabilidad Objetiva, de acuerdo a lo que se ha establecido en diversas ramas del Derecho al respecto, entre ellas el Derecho del Consumidor con la Ley de Protección al Consumidor.

[12] Reglamento del Sistema de Pagos, aprobado por la Junta Directiva del Banco Central de Costa Rica en la sesión 5368-2008, publicado en el diario oficial La Gaceta 53 del 14 de marzo del 2008.

En la investigación se desarrolla lo relacionado con el Comercio Electrónico y los Delitos Informáticos, analizándose los elementos que componen el Comercio Electrónico, entre ellos la Banca por Internet. En este tema en particular, se da una amplia explicación de este novedoso mecanismo y se desarrolla el punto de los contratos por medios electrónicos. Además, se desarrollan a profundidad los tipos de delitos informáticos que más han afectado a esta actividad así como las medidas de seguridad recomendadas y adoptadas por las entidades bancarias.

Como último punto, en el capítulo tercero se analiza cómo ha sido manejado el conflicto de la responsabilidad bancaria frente al cliente por delitos informáticos, es por ello que se explica brevemente el funcionamiento y desarrollo en Costa Rica del Derecho del Consumidor, así como su posición sobre el tema y los planteamientos que han sido puestos en práctica en procura de sus derechos, por ejemplo, el Proceso Colectivo entablado por la ACL en representación de múltiples víctimas. Se da una descripción de la posición de los bancos, en el sentido de desvirtuar la existencia de responsabilidad civil de las entidades bancarias.

Por otra parte, se incorporan los argumentos determinados por los órganos que han resuelto el conflicto: el Tribunal Contencioso Administrativo y la Sala Primera. Por

último se agrega un criterio o posición personal sobre el tema que incluye una serie de propuestas y perspectivas propias de la sustentante.

METODOLOGÍA

Para la investigación del tema planteado se implementó en gran medida la investigación documental[13], ya que en su mayoría las fuentes de investigación a utilizar las constituyeron los documentos. También se hizo necesario el uso, de manera bastante amplia, de la investigación de campo; primordialmente, de la realización de entrevistas y encuestas.

Ahondando en lo anterior, con el término "documentos" se hace referencia a los textos desarrollados por la Doctrina, es decir, libros, artículos especializados en la materia, ensayos, tratados, entre otros.

De igual manera, se examinará con detalle diversos textos de Derecho Positivo. Dentro de los mismos se incluye todo lo relativo a la legislación: la Constitución Política,

[13] GALLARDO MARTÍNEZ, Helio. (2008). *Elementos de investigación académica.* San José, Costa Rica. Primera edición, EUNED.

leyes, reglamentos, entre otros. Igualmente, se incorporan dentro del análisis, las resoluciones emanadas de órganos jurisdiccionales.

Para explicar una norma jurídica, se tomó en cuenta los diversos esquemas metodológicos que han sido utilizados en la interpretación del derecho escrito. Dichos métodos son conocidos en la función hermenéutica como: el método literal-gramatical, los métodos psicológico-voluntaristas, los métodos lógico-dogmáticos, métodos axiológico-teleológicos, o bien, métodos realista-sociológicos, entre otros[14].

En esta investigación se utilizó el método deductivo, por medio del cual, al partir de nociones generales se arriba a conclusiones específicas. También fue necesario exponer en primera instancia sobre el análisis de los diversos conceptos que integran el objeto de estudio. Por esta razón se empleó el método descriptivo, que permite brindar al lector un marco conceptual que le permita comprender cuál es el estado de la cuestión existente en la materia.

Posteriormente, se entró a un nivel de comprensión, en donde se verificó la hipótesis, una vez analizados todos los objetivos propuestos y cuando la investigación se tenga por consumada, para culminar con la formulación de conclusiones y propuestas.

[14] Nomenclatura adoptada en HABA MÜLLER, Enrique Pedro. (1972). *Esquemas metodológicos en la interpretación del derecho escrito. en Cuadernos de Filosofía del Derecho.* Caracas, Venezuela. Universidad Central de Venezuela.

CAPÍTULO PRIMERO

Responsabilidad Civil: ¿Qué tipos existen y de qué manera se incurre en ella?

Aspectos Generales y tendencias legislativas

Dentro del marco de la responsabilidad civil se encuentran dos vertientes diferenciadoras que definen el tipo de responsabilidad en que se incurre cuando se produce un daño, esta distinción se hace dependiendo de si existe o no una relación contractual preestablecida entre las partes o si por el contrario, la obligación de resarcir se deriva de una actividad en la que no se contaba con un vínculo contractual previo.

SECCIÓN I

TIPOS DE RESPONSABILIDAD

1.1 RESPONSABILIDAD CIVIL CONTRACTUAL

En este tipo de responsabilidad se da la existencia de un vínculo entre los sujetos involucrados. Su finalidad es garantizar al sujeto el equivalente económico de su prestación, de una actividad de cooperación de otro sujeto[15].

La Responsabilidad Contractual funciona como una garantía ante el incumplimiento de lo que fue previamente pactado entre las partes. Surge una vez que no se ha hecho efectivo tal y como se pactó el cumplimiento de la prestación debida, pero para valorarse ese incumplimiento no solamente se toma en cuenta lo que el contrato indica, sino también lo que la Ley determina, por ejemplo, la buena fe, principio bajo el cual deben actuar las partes.

[15] PÉREZ VARGAS, V. op. cit. P. 388

Las partes contractuales deben cumplir con una serie de deberes, que aseguran el adecuando cumplimiento del contrato, y dependiendo del tipo de servicio que se preste, así deben ser las obligaciones que se deben llevar a cabo.

Así mismo, deben excluirse todas aquellas cláusulas que resulten inadmisibles por dolosas, abusivas o contrarias a la equidad contractual que la buena fe defiende, por ejemplo aquellas que pretendan excluir la responsabilidad de una de las partes en cuanto a un daño o incumplimiento que le sea imputable, ya sea por la Ley o bien porque forma parte connatural del contrato que le vincula.[16]

Una cláusula limitativa de responsabilidad no es sólo aquella que reduce o anula el ámbito de eventos o supuestos en que una de las parte a de responder, sino aquellas otras que implican reducir plazos de reclamación, excluir supuestos que de ordinario han de cubrirse o reducen el alcance de la reparación del daño injustificadamente.[17]

[16] OROZCO PARDO, Guillermo (1998). *Responsabilidad Civil en materia de informática*. Jornadas marco legal y deontológico de la informática: actas volumen I. España. No. 19-20-21-22. P. 159.

[17] OROZCO PARDO, G. op. cit. 159.

1.2 RESPONSABILIDAD CIVIL EXTRACONTRACTUAL

En este tipo de Responsabilidad Civil no hay un vínculo preexistente entre quien configura el daño y el sujeto dañado. La responsabilidad se genera cuando una persona violenta un interés que es jurídicamente relevante y no existe una relación jurídica entre esta persona y a quien se le produce un daño. Se interpreta que para que se configure la responsabilidad extracontractual, debe hacerse faltado al deber genérico de la diligencia en la vida social, siendo definida ésta como una diligencia media, la que todo hombre medio pueda ejecutar.

La fuente de la Responsabilidad Extracontractual se encuentra en los delitos y los cuasidelitos, siendo el primero un hecho típico, antijurídico y culpable que produce un resultado dañoso, con un comportamiento querido por el que produce el daño, existe dolo; en los segundos son los comportamientos no queridos pero que igualmente producen un resultado dañoso, es una conducta culposa. Para ambas situaciones, la consecuencia civil que deviene es el resarcimiento de este daño.

La legislación civil costarricense ha estipulado de forma general en su artículo 1045 del Código Civil el principio de Responsabilidad Civil Extracontractual, sin embargo se ha considerado que el citado artículo no incluye los supuestos de la Responsabilidad Objetiva.

Este principio, según considera el Dr. Víctor Pérez Vargas, es más bien de orden constitucional, encontrándose en el artículo 41 de la Constitución Política[18]. En Costa Rica, el régimen de Responsabilidad Objetiva no ha sido fijado de manera general, y se aplica en los casos en que la ley específicamente lo haya determinado, un ejemplo de ello es el artículo 35 de la Ley 7472: Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

[18] Artículo 41 de la Constitución Política: "*Ocurriendo a las leyes, todos han de encontrar reparación para las injurias o daños que hayan recibido en su persona, propiedad o intereses morales. Deberá hacérseles justicia pronta y cumplida, sin denegación y en estricta conformidad con las leyes*".

SECCIÓN II

CRITERIOS DE IMPUTACIÓN

Tanto para el análisis de la responsabilidad civil extracontractual como para la responsabilidad civil contractual, deben tenerse presentes los criterios de imputación existentes, a saber: la responsabilidad subjetiva y la responsabilidad objetiva. Esto sobre todo para la determinación de la carga de la prueba.

2.1 RESPONSABILIDAD SUBJETIVA:

Para este criterio de imputación el elemento culpa es indispensable para su configuración. Así, es preciso que si se ha producido un daño, éste pueda ser imputable a un sujeto o agente productor, ya sea por dolo o culpa (omisión de la diligencia exigible: deber de actuar en sociedad como un buen padre de familia, negligencia).

Tiene además, como requisito que el sujeto que alega el perjuicio pruebe la existencia de la culpa por parte del sujeto que lo perjudica, para que así se haga efectiva la responsabilidad de este último.

En cuanto a la responsabilidad contractual, existe una presunción de culpa para quien no ha cumplido su obligación. Únicamente si se prueba por parte del deudor que el incumplimiento o el atraso no le son imputables ya sea por caso fortuito o fuerza mayor, es que no es efectiva esta presunción.

En la responsabilidad extracontractual, no existe esta presunción, y quien pretende el resarcimiento es quien debe probar la culpabilidad de quien figura como el productor del daño, demostrando que su actuar fue la causa directa del daño, según el principio general de que quien intente una acción debe probar los hechos en que se fundamente.

Existe otra diferencia entre la responsabilidad contractual y la extracontractual con respecto a los daños imprevisibles. Para la primera, se ha indicado que de no existir dolo no hay responsabilidad en cuanto a los daños imprevisibles, se limita entonces la responsabilidad a aquellos daños que podían preverse en el momento de adquirir la obligación. Sin embargo, en la segunda, se comprenden los daños imprevisibles.

La responsabilidad extracontractual, dentro de la doctrina de la responsabilidad subjetiva, contiene tres elementos: daño causado, la antijuricidad y la culpabilidad. Así, para que una persona sea responsable extracontractualmente debe comprobarse la existencia de un daño y de su causa, que éste sea antijurídico y que además le sea imputable.

En la responsabilidad subjetiva prima el principio de causalidad. Este se refiere a la relación de causalidad entre el hecho y el daño producido, en donde no solamente se constituye la obligación de resarcir con la presencia del daño causado por un acto antijurídico imputable por dolo o culpa a un sujeto, sino que además debe existir una conexión, un vínculo entre ese hecho y el daño. Para que una persona sea tenida como responsable de un hecho, debe determinarse de manera inequívoca que su actuación fue la que provocó el daño, y por ello lo debe de reparar. De no demostrarse este nexo, entonces no podría existir responsabilidad.

Este principio se ubica dentro del derecho civil costarricense en el artículo 704 del Código Civil, que se refiere específicamente a la responsabilidad civil contractual, aunque ha sido utilizado, a falta de otra norma, en la responsabilidad civil extracontractual.

El nexo causal se rompe cuando interviene un elemento externo que puede ser el caso fortuito o la fuerza mayor, entendidos como eventos imprevisibles o inevitables, no imputables al sujeto, la acción de un tercero y la conducta del propio perjudicado (culpa de la víctima). Estas dos últimas deben ser valoradas para conocer cual es su grado de participación en el evento dañoso.[19]

2.2 RESPONSABILIDAD OBJETIVA

En cuanto a la tesis de la Responsabilidad Objetiva, se tiene como superado el principio de la culpa, sin que se hagan necesarios los elementos antes descritos para que se configure la obligación de reparación. Dentro de esta teoría sólo sería necesaria la existencia de un daño y de una conducta o actividad que sirva como criterio de imputación de ese daño. Así, por ejemplo, en la responsabilidad objetiva se tiene el daño y la creación de un riesgo como elementos del supuesto.[20]

[19] DÍAZ DE LEZCANO, I. citado por OROZCO PARDO, Guillermo (1998). *Responsabilidad Civil en materia de informática*. Jornadas marco legal y deontológico de la informática: actas volumen I. España. No. 19-20-21-22. P. 152.
[20] PÉREZ VARGAS, V. op.cit. P. 394

La responsabilidad objetiva se basa en el resultado y la actividad: toda actividad que genere un riesgo y, por lo tanto, sea susceptible de producir un daño, debe contar con la consiguiente obligación de responder si éste se produce.[21]

La Sala Primera ha dicho que la Responsabilidad Objetiva*: "Es el resultado de una revisión del instituto de la responsabilidad que vino a ser necesaria cuando se tomó conciencia que el molde de la culpa era estrecho para contener las aspiraciones de justicia que clamaban en un mundo cada vez más complejo. Exigencias de la realidad, la multiplicación de los peligros y daños propios de la vida moderna, justificaron que en determinadas situaciones la responsabilidad fuese tratada como un crédito de la víctima que el demandado debía desvirtuar. La teoría del riesgo, según la cual quien ejerce o se aprovecha de una actividad con elementos potencialmente peligrosos para los demás, debe también soportar sus inconveniencias, permeó la mayor parte de las legislaciones y en el caso de Costa Rica origina el párrafo V de comentario. Esta teoría es también denominada del daño creado, cuyo paradigma de imputación, según lo refiere el Profesor Alterini, '...estriba en atribuir el daño a todo el que introduce en la sociedad un elemento virtual de producirlo...ella, agrega, ...'prescinde de la subjetividad del agente, y centra el problema de la reparación y sus límites en torno de la causalidad material, investigando tan solo cual hecho fue, materialmente, causa del efecto, para atribuírselo sin más. Le*

[21] OROZCO PARDO, Guillermo (1998). <u>*Responsabilidad Civil en materia de informática*</u>. Jornadas marco legal y deontológico de la informática: actas volumen I. España. No. 19-20-21-22. P. 148.

basta la producción del resultado dañoso, no exige la configuración de un acto ilícito a través de los elementos tradicionales..' (Alterini, Atilio. Responsabilidad Civil, Abeledo Perrot, III Edic., Buenos Aires, 1987, pág 106)."[22]

Dentro de la Responsabilidad Objetiva, no se le imputa al sujeto activo un comportamiento o un hecho, sino que basta con que éste produzca un daño para que sea responsable. Por ello se denomina objetiva, pues solamente se valora el daño causado, sin considerar lo subjetivo de las circunstancias, si hubo o no culpabilidad del sujeto activo y se le conoce también como responsabilidad sin culpa.[23]

Este tipo de Responsabilidad se basa en lo que se denomina la Teoría del Riesgo creado, que consiste en que la persona que se beneficia por la explotación de un bien que constituye un peligro o riesgo para la sociedad debe hacerle frente a los daños que con su explotación ocasione, sin tomar en cuenta la antijuricidad o la culpabilidad, pues aunque actúe de forma diligente si no se evita el daño, no puede dejarse éste sin resarcimiento. Se trata de la realización de actividades que son lícitas o permitidas, pero que obligan al resarcimiento de los daños que puedan producir al efectuarse. Si la actividad es creadora de riesgos y produce un daño este daño debe resarcirse, y la teoría de la culpabilidad no

[22] Sala Primera de la Corte de Justicia. Sentencia 61-1997 de las catorce horas cincuenta minutos del diecinueve de junio de mil novecientos noventa y siete.
[23] MONTERO PIÑA, Fernando (1999). *Obligaciones*. San José, Costa Rica. Premiá Editores. P.327

es suficiente para abarcar este tipo de casos, por lo que se hace necesario el empleo de la Responsabilidad Objetiva.

La Responsabilidad Objetiva responde a las necesidades de indemnización surgidas sobre todo con la industrialización, pues cada vez se hacía más difícil resarcir los daños producidos en las empresas o por la utilización de máquinas con el esquema de responsabilidad existente, es decir, la responsabilidad subjetiva, es por ello que se busca una alternativa que garantice la indemnización de las víctimas.

Cada vez más, como efecto colateral al progreso técnico científico imperante, se producen una serie de riesgos o situaciones peligrosas que implican una extensión de la obligación de resarcir por el daño producido. Así, se ha empleado la solución de crear una serie de seguros de responsabilidad civil, lo que funciona como un recurso para defender el patrimonio de quien explota un bien y crea un riesgo, ya que al no poder evitarse el daño, se debe enfrentar la indemnización, y con los seguros la traslada al ente asegurador.

En la Responsabilidad sin culpa la carga de la prueba se traslada al creador del riesgo, y la única forma que tiene para eximirse de responsabilidad es probando la existencia de fuerza mayor o culpa de la víctima. Aquí no interesa si en su actuar tuvo en cuenta la debida diligencia. Así, para don Víctor Pérez Vargas, "*la responsabilidad objetiva*

se resume en una ventaja a favor del lesionado, que significa una parcial inversión de la carga de la prueba, en el sentido de que éste queda exonerado de la carga de probar la culpa (culpa o dolo) del causante del daño y vano sería el intento de probar su falta de culpa, a diferencia de lo que ocurre en los supuestos de responsabilidad subjetiva".[24]

La jurisprudencia nacional ha establecido una serie de presupuestos para que se configure la Responsabilidad Objetiva:

> *"Para la configuración de este tipo de responsabilidad deben darse los siguientes componentes: a) el empleo de cosas que conlleven peligro o riesgo; b) causar un daño; y c) la relación o nexo de causa efecto entre el hecho y el daño. Finalmente, es importante mencionar que, dentro de esta temática, opera una parcial inversión de la prueba, en el sentido de que el lesionado queda exonerado de la carga de probar la culpa o dolo de quien provocó el daño. En consecuencia, le atañe a la persona física o jurídica a quien se le atribuye la responsabilidad, demostrar que los daños se produjeron por fuerza mayor o por culpa de la víctima."*[25]

[24] PÉREZ VARGAS, V. op. cit. P. 417
[25] Sala Primera de la Corte Suprema de Justicia. Sentencia 376-F-99 de las catorce horas cuarenta minutos del nueve de julio de mil novecientos noventa y nueve.

Así, hace falta que se cumplan tres elementos o presupuestos para que se concrete la Responsabilidad Objetiva:

1. **Un acto u omisión:** con respecto a los actos, se trata de una conducta voluntaria, que puede ser incluso lícita, pero que excede de los límites racionales del riesgo y por lo tanto genera una situación de peligro, y en caso de que se materialice la situación riesgosa se genera la obligación de resarcimiento de los daños producidos como consecuencia de estos actos. En el mismo sentido se entiende la omisión, en el tanto ese no hacer genere un riesgo, pues se omite una conducta que debió llevarse a cabo, es decir una actuación debida, debe responderse por las consecuencias que genere dicha omisión.

2. **El daño**: supone una pérdida o lesión, ya sea económica o física, que sufre un sujeto como consecuencia de un acto u omisión. Este daño produce consecuencias resarcibles a nivel patrimonial y también puede indemnizarse a por daño moral si se demuestra que se produjo una lesión en este sentido.

3. **El nexo causal:** *"Entre el daño y la acción debe haber un vínculo de causalidad en la medida en que ésta ha sido la causa que origina la lesión o*

menoscabo. (…)"[26]. En los casos en que se alega la existencia de Responsabilidad Objetiva debe cumplirse de forma obligatoria con este requisito, debe concretarse ineludiblemente la causalidad entre la actividad riesgosa y el daño, es decir que el segundo sea consecuencia inmediata y directa del primero. Para cada situación debe examinarse que la relación de causalidad entre el hecho que es fuente de riesgo o peligro y el daño sufrido. Si la relación entre hecho y daño se verifica nace la obligación de resarcimiento, de modo tal que no puede presumirse el nexo causal.

Existe en el tema del nexo causal dos posiciones. La primera es la denominada Teoría de la Equivalencia, según la cual se considera causa del daño toda acción que contribuye al resultado lesivo de suerte que, sin ella, no se habría producido[27]. Por otra parte, se encuentra la Teoría de la Causalidad Adecuada, que es la que rige en nuestro país, tal y como ha sido fijado jurisprudencialmente, y que consiste en la verificación de la existencia de un vínculo causal entre el hecho y el daño. Este vínculo debe ser adecuado y suficiente, de manera que la causa sea apta para producir aquel daño que se le atribuye; bajo esta teoría, el resultado ha de ser una consecuencia natural, adecuada y suficiente de la acción[28].

[26] OROZCO PARDO, G. op. cit. P. 150
[27] Ibídem.
[28] Ibídem, P.P. 150 y 151.

La única manera de romper ese nexo de causalidad es que el demandado demuestre que existió fuerza mayor o culpa de la víctima. En estos términos se desarrolla la Teoría de la Ajeneidad, bajo la cual sólo se libra de responsabilidad aquel que demuestra que ha sido ajeno al daño, es decir, que se debió a una causa extraña no imputable al demandado. También, nuestra legislación admite la Teoría de la imputación objetiva, la cual sostiene que aquellas conductas, ya sean activas u omisivas, que no eleven el riesgo normal a que ordinariamente está expuesto un bien jurídico, no se le pueden atribuir al autor del comportamiento dado.

En la actualidad, la doctrina más moderna defiende la idea de un único concepto de responsabilidad que se identifica con la idea de tener que cumplir una obligación o de compartir las consecuencias de esa obligación[29]. Existe por lo tanto, una tendencia objetivadora de la responsabilidad civil. La idea es asegurar la indemnización de las víctimas, más allá de cualquier aspecto subjetivo de la conducta creadora del daño.

En los supuestos en que concurren conductas de varios sujetos, sin que pueda determinarse con claridad quién fue el responsable directo del daño, se ha consagrado un sistema de solidaridad, esto cuando no es posible realizarse una imputación adecuada. Esto es así porque lo prioritario es asegurar la reparación. No es una culpa compartida (in

[29] Ibídem, P.148

vigilando-in eligendo), sino que se busca que la víctima no soporte sola las consecuencias del daño causado. Para establecer la responsabilidad en sede judicial, la acción se dirige contra todos los posibles autores, pues existe una pluralidad de obligaciones que cada uno debe cumplir.

SECCIÓN III

LA RESPONSABILIDAD OBJETIVA, MANIFESTACIONES Y ENFOQUE JUDICIAL

3.1 ANÁLISIS JURISPRUDENCIAL DE LA SALA PRIMERA SOBRE RESPONSABILIDAD OBJETIVA

La teoría del riesgo creado, recogida en la Responsabilidad Objetiva, ha permeado la jurisprudencia patria desde años atrás. Este concepto ha ido adquiriendo fuerza con el tiempo, ya que como se comentó anteriormente, los ordenamientos jurídicos de distintos países, sin que Costa Rica sea la excepción, han ido adquiriendo dentro de su legislación la Responsabilidad Objetiva con el fin de cubrir aquellas fuentes de riesgo que puedan generar daños a las personas y que éstas reciban una efectiva reparación o resarcimiento.

La jurisprudencia que puede encontrarse al respecto es amplia y abundante, dentro de las que se pueden encontrar resoluciones de vieja data que plasman los primeros criterios de los juzgadores en situaciones que permiten la aplicación de este instituto. Para la

presente investigación se eligieron resoluciones recientes, pero que reflejan el núcleo principal de la visión actual sobre la Responsabilidad sin culpa.

Las sentencias que tienen que ver con Responsabilidad Objetiva han abordado distintos temas, por ejemplo, la responsabilidad por productos defectuosos, por defectos en los servicios, por robo de vehículos en estacionamientos de locales comerciales o entidades que ofrecen un servicio, por faltar a los deberes de vigilancia y cuidado y provocar accidentes, por omisión en la seguridad, por lesiones a la salud pública o a los recursos naturales, entre otros. De cada uno de estos temas se han dado numerosas sentencias, por lo que se hace necesario seleccionar las más representativas y extraer las principales ideas que en torno a este tema se han generado.

La jurisprudencia ha definido la responsabilidad objetiva y sus alcances en diversas resoluciones, pero el argumento ha sido reiterado en los siguientes términos:

> *"En lo tocante al régimen objetivo de responsabilidad, esta Sala en el fallo no. 376-f-99 de las 14 horas 40 minutos del 9 de julio de 1999, indicó que "preceptúa lo que la doctrina ha denominado responsabilidad objetiva o por riesgo creado. En ella, se prescinde del elemento culpa como criterio de imputación, enfocándose en una conducta o actividad de un sujeto físico o*

jurídico, caracterizada por la puesta en marcha de una actividad peligrosa, o la mera tenencia de un objeto de peligro. El elemento de imputación de esta responsabilidad es el riesgo creado, o la conducta creadora del riesgo. Por ello, se afirma, la noción de riesgo sustituye los conceptos de culpa y antijuricidad. (…) La responsabilidad objetiva reside en el hecho de que, aquél que, para su propio provecho, crea una fuente de probables daños y expone a las personas y bienes ajenos a peligro, queda obligado si el daño se verifica. Para determinar esta responsabilidad, debe existir un nexo de causalidad entre la actividad riesgosa puesta en marcha y el daño ocasionado. Nuestra jurisprudencia, desde épocas pretéritas, ha reconocido este tipo de responsabilidad. Sobre el particular, pueden consultarse las sentencias de la antigua Sala de Casación número 97 de las 16 hrs. del 20 de agosto de 1976; y de esta Sala, entre otras, las números 26 de las 15:10 hrs. del 10 de mayo de 1989; 263 de las 15:30 hrs. del 22 de agosto de 1990; 354 de las 10 hrs. del 14 de diciembre de 1990; 138 de las 15:05 hrs. del 23 de agosto de 1991; 112 de las 14:15 hrs. del 15 de julio de 1992; y, 61 de las 14:50 hrs. del 19 de junio de 1996. En consecuencia, la responsabilidad objetiva emerge de la realización de actividades lícitas o autorizadas, pero que constituyen una fuente de riesgo (…) En el presente caso surge la responsabilidad objetiva, cuyo punto de partida no es la acción del sujeto sino más bien el desarrollo de

actividades industriales, comerciales, agrícolas que aunque lícitas, son causas generadoras de riesgo y fuente potencial de daños. Su fundamento no es subjetivo, sino más bien objetivo en la medida que el interés central no es sancionar o castigar, sino reparar."[30]

Este criterio ha sido el marco de referencia para los juzgadores cuando se enfrentan a un caso en el que se alega la responsabilidad objetiva o sin culpa. En concordancia con lo anterior, una de las resoluciones más conocidas es la número 000646-F-2001 de la Sala Primera de la Corte Suprema de Justicia (en adelante Sala Primera), dada a las dieciséis horas cuarenta y cinco minutos del veintidós de agosto del dos mil uno, y tiene que ver con una lesión sufrida por un consumidor con una botella de vidrio defectuosa que estalló cuando éste la quiso abrir, lastimándole su ojo.

En esta sentencia se demostró el nexo causal entre la lesión sufrida por el consumidor y el estallido de la botella, que venía defectuosa y por esta razón provocó el daño. En concordancia con la teoría del riesgo creado, la empresa debe indemnizar al consumidor que se vio afectado a causa de su producto, sin que se haya demostrado eximente alguna de responsabilidad.

[30] Tribunal de Casación Penal. Sentencia 0493-2004 de las diez horas con once minutos del 20 de mayo del 2004.

Este criterio es interesante pues marca un precedente sobre la responsabilidad de los empresarios con respecto a sus productos. Si por causa de alguno de los servicios que los productores estén brindando se llega a provocar un daño, en este caso una lesión que afecta el bien jurídico salud, derecho fundamental, se origina en el productor la obligación de indemnizar al consumidor. Por lo tanto, los productos que se encuentren en el mercado deben cumplir con una serie de requisitos que los haga seguros para su consumo, de no ser así, tal y como se hizo en esta sentencia, se obliga al resarcimiento de los daños.

En el mismo sentido se ubican las resoluciones 000575-F-03 de las diez horas del diecisiete de octubre del dos mil tres de la Sala Primera y la 035-2009 de las nueve horas cuarenta minutos del veintiuno de enero del dos mil nueve del Tribunal Segundo Civil de San José, Sección Primera. En ambas sentencias los consumidores se vieron lesionados en los locales comerciales en los que se encontraban como producto del descuido de los empleados del lugar. En la primera de las resoluciones mencionadas, la actora sufrió luxación y fractura de las últimas vértebras coccígeas como producto de una caída en un restaurante en el que había un producto líquido y aceitoso derramado en el piso. En la segunda sentencia, la actora sufrió una caída cuando se encontraba en un supermercado y se tropezó con unas cajas que estaban mal colocadas en un pasillo, al caer sus rodillas impactaron en el suelo y se produjo una herida al quebrarse una botella que traía en sus

manos. Este hecho le ocasionó lesiones y una pérdida del 4% de la capacidad general orgánica.

De nuevo, para ambos casos, se analiza el nexo causal y se determina que las lesiones sufridas por las actoras son consecuencia directa del servicio brindado por los demandados, pues deben tener el cuidado necesario para no provocar accidentes en sus usuarios. En los casos en estudio, las consumidoras se vieron perjudicadas con motivo del servicio que se estaba brindando y que estaban utilizando, lo que encaja dentro del artículo 32 de la Ley de Protección al Consumidor.

Es menester recordar en este punto que para que la Responsabilidad Objetiva sea aplicable a una situación específica ésta debe estar tipificada, es decir, debe haberse establecido una normativa que indique que para ese caso aplica el régimen de la responsabilidad por riesgo creado. Así, se han dado situaciones en las que se alega la existencia de la Responsabilidad Objetiva pero ha sido necesario evaluar las condiciones fácticas específicas para poder determinar si ésta le es aplicable o no.

Dentro de este tipo de casos se encuentran las sentencias que a continuación se examinarán. La primera de ellas es la sentencia 00617-09 del Tribunal de Casación Penal[31], en la que se cuestiona la responsabilidad existente de un vehículo utilizado para fletes de materiales que ocasionó un accidente y provocó lesiones. En este fallo se determinó que de acuerdo al artículo 187 de la Ley de Tránsito 7331 vigente, que establece los supuestos en los cuales aplica la responsabilidad solidaria, existe responsabilidad objetiva en este caso pues se trata de un vehículo que es utilizado para la explotación comercial, con fines de lucro y provocó un daño, por lo que encaja en el inciso b) del citado artículo.

La jurisprudencia ha dicho que los párrafos cuarto y quinto del artículo 1048 de Código Civil se refieren a responsabilidad objetiva[32]. Incluso, en el cuarto párrafo se establece de forma expresa que no es admisible como eximente de responsabilidad el argumentar que el daño no pudo ser evitado incluso con el empleo de la debida diligencia, en los casos que ahí se indican. La responsabilidad sin culpa recae sobre los empresarios de establecimientos peligrosos y los que se dedican a la explotación de medios de transporte, claro está una vez que se haya comprobado la existencia de un nexo causal.

Dentro de este mismo orden de ideas, se hace ahora alusión a la resolución 00840-08 también del Tribunal de Casación, en donde se aclara que es viable imponer una

[31] Tribunal de Casación Penal. Sentencia 00617-09 de las diez horas quince minutos del doce de junio del dos mil nueve.
[32] Así lo manifiesta el jurista Víctor Pérez Vargas en PÉREZ VARGAS, Víctor (1994). op. cit. P. 416

condena civil en una causa penal aún y cuando en lo penal se haya absuelto al imputado, pues la responsabilidad civil no se deriva necesariamente de la responsabilidad penal[33]. La conducción de vehículos es una actividad que es considerada como riesgosa, sin embargo, es una actividad permitida, siempre y cuando no se excedan los límites permitidos de riesgo.

Así, no por el sólo hecho de realizar una actividad riesgosa se incurre en responsabilidad objetiva, pues la acción debe estar primeramente tipificada como tal y debe excederse del riesgo permitido. Por ejemplo, en el caso de accidentes de tránsito, debe tomarse en cuenta que la conducción es una actividad riesgosa permitida, por lo que debe examinarse casuísticamente, si en efecto el daño se provocó por una extralimitación de ese riesgo permitido.

Este principio queda plasmado en la resolución 383-2005 de la Sala Tercera[34], en donde expresamente se manifiesta que de acuerdo a la Teoría de la Causalidad adecuada, la vinculación causal debe existir entre la actividad que desencadena el riesgo y el daño sufrido, de modo que la obligación de resarcir se presenta si el daño se verifica como consecuencia o concreción de la actividad que es fuente de peligro o riesgo. No debe

[33] Para ahondar más en el tema véase SANABRIA ROJAS, Rafael Ángel (2008). *Reparación civil en el proceso penal*. San José, Costa Rica. EDITORAMA S.A.
[34] Sala Tercera de la Corte Suprema de Justicia. Sentencia 00383-2005 de las ocho horas cuarenta minutos del trece de mayo del dos mil cinco.

presumirse el nexo causal por el solo hecho de tratarse de vehículos y que exista una lesión, la causa debe ser inmediata y directa en relación con el daño producido.

Otro tema interesante que se ha permeado por la Responsabilidad sin culpa es el del derecho al ambiente y los recursos naturales. En varias resoluciones se ha dejado claro que la contaminación o daño de recursos naturales o a bienes ajenos a través de actividades tipificadas como riesgosas, por ejemplo, las quemas controladas generan responsabilidad objetiva del productor de la actividad. En el tema de incendios o quemas controladas, a pesar de tratarse de una actividad lícita, de contar con los permisos para realizarlas del Ministerio de Agricultura y Ganadería e incluso si se tomaron todas las previsiones del caso, pero aún así se provocó un daño, se incurre en responsabilidad objetiva, criterio que ha sido esbozado por el Tribunal Agrario de San José[35].

Por otro lado, se tiene otro tipo de casos que han definido las obligaciones de los comerciantes o productores como parte de una cadena contractual y de acuerdo al régimen de responsabilidad establecido en la Ley 7472. Uno de estos puntos ha sido el del robo de vehículos en locales comerciales o estacionamientos disponibles como parte de un servicio ofrecido al consumidor. Sobre este particular existe abundante jurisprudencia, pero todas concuerdan en el sentido de que los estacionamientos son espacios dispuestos

[35] Tribunal Agrario del Segundo Circuito Judicial de San José. Sentencia 00815-2003 de las catorce horas y cincuenta y cinco minutos del dieciséis de diciembre del dos mil tres.

para el cliente y forman parte del servicio ofrecido, son un atractivo para los clientes y por lo tanto se tienen como un adicional al bien ofrecido.

Se toman como ejemplo, dentro del análisis jurisprudencial, las resoluciones 000467-F-S1-2008 de las catorce horas con veinticinco minutos del cuatro de julio del dos mil ocho dictada por la Sala Primera, la 668-F-08 de las siete horas treinta minutos del ocho de agosto del dos mil ocho del Tribunal Primero Civil de San José y la 0258-09 de las dieciséis horas cincuenta minutos del treinta y uno de julio del dos mil nueve del Tribunal Segundo Civil de San José, Sección Segunda.

En estas sentencias se sustenta el criterio de que los estacionamientos de los establecimientos comerciales o de servicios son un mecanismo para atraer clientes y por lo tanto forman parte del negocio, por lo que en caso de darse un daño a los consumidores, es la empresa o el oferente del servicio quien debe responsabilizarse por ellos, en el tanto se encuentra en la obligación de brindarle protección y seguridad a éste.

> *"(…) si la demandada como accesorio o agregado al servicio principal que ofrece al consumidor en su negocio de supermercado ofrece además el servicio de parqueo de vehículos gratuito a sus clientes, es responsable también por los riesgos que este servicio conlleva, entre ellos el de robo de*

vehículos de consumidores que se produzcan en el lugar, salvo que demuestre que es ajena al daño, cosa que no ha demostrado en autos."[36]

Los argumentos de la contraparte demandada han ido enrumbados en traspasar la responsabilidad a terceros o incluso al propio consumidor. Se ha dicho, por ejemplo, que existe culpa de la víctima ya que el usuario no dotó a su vehículo de sistemas de seguridad antirrobo o de seguros, de modo que estas circunstancias median como concausas para la generación del daño, eximiendo parcialmente de responsabilidad. Sin embargo, en primera instancia, criterio que fue confirmado por la Sala Primera, se consideró que: *"No cabe introducir como antecedente, según se pretende, vía interpretación del artículo 35 citado, que en casos como este es causa eximente de responsabilidad de las empresas de servicio, o de disminución de ella, el hecho que el cliente o consumidor no haya proveído a su vehículo, para evitar el robo, de medidas de seguridad como las señaladas por la apelante en sus agravios, y lo deje estacionado en esas condiciones en parqueos de tales empresas, mientras realizan sus compras en ellas, pues si se procede de esa forma equivaldría a echar por tierra todo el espíritu de protección al consumidor que permea la ley ya citada, en perjuicio de éste y en beneficio de las grandes empresas. Los*

[36] Sala Primera de la Corte Suprema de Justicia. Sentencia 000467-F-S1-2008 de las catorce horas veinticinco minutos del cuatro de julio de dos mil ocho.

consumidores no están obligados a tomar tales medidas, pues sería exigirles un deber de cuidado excesivo."[37]

En la sentencia citada del Tribunal Primero Civil de San José con número 668-F-08 en la que una alumna de una universidad sufrió el robo de su vehículo en el parqueo de la institución se alegó por la parte demandada, que en el parqueo se pusieron rótulos indicando que la institución no se hacía responsable por robos, según lo dispone el reglamento interno de la misma. En un primer análisis, el Tribunal determinó que el ser estudiante de ese centro universitario la acreditaba como consumidora, por lo que en este caso resultan aplicables las reglas de la Ley de Protección al Consumidor, en específico el artículo 35 que establece la responsabilidad objetiva en materia del consumidor.

Además se determinó, en concordancia con el criterio de la Sala Primera, que la culpa del agente no es un elemento esencial para darle origen a la responsabilidad, en razón de lo dispuesto en el artículo mencionado, el cual señala que los establecimientos comerciales los cuales ofrezcan parqueo a sus clientes, deben proteger los vehículos ante posibles daños, sean causados por personas ajenas o no a la organización interna de la empresa y que de darse surge la obligación de indemnizar. Cabe así la responsabilidad

[37] Ibídem.

objetiva del comerciante cuando el consumidor es lesionado en razón del bien o servicio prestado.

> *"El contenido del reglamento y el rótulo exhibido en la entrada, por tratarse de una responsabilidad objetiva por imperativo del numeral 35 de la citada ley, no figuran como eximentes para evitar el pago de la indemnización. Como empresa que presta servicios educativos al consumidor, no puede ignorar lo dispuesto en la normativa especial, de ahí que tampoco sea posible exonerarla de las costas. (…)"*[38]

La Sala Primera también ha dado su criterio con respecto a la colocación de rótulos o entrega de tiquetes con el objetivo de exonerarse de responsabilidad, y ha indicado que el parqueo forma una unidad con el servicio prestado que originó su uso, por lo que la advertencia mediante entrega de tiquetes y letreros colocados en paredes o lugares visibles, en el sentido de que la empresa no se hace responsable por los daños sufridos, no es una eximente de responsabilidad. La empresa debe responder por más que advierta lo contrario pues los derechos de los consumidores son irrenunciables.

[38] Tribunal Primero Civil de San José. Sentencia 668-F-08 de las siete horas treinta minutos del ocho de agosto del dos mil ocho.

También ha dicho la Sala Primera que el hecho que el parqueo sea un servicio gratuito no implica que no pueda imputársele responsabilidad por daños al comerciante, pues tal y como ya se mencionó, el estacionamiento forma parte del servicio prestado y el no responsabilizarse por las lesiones causadas al usuario en el ejercicio de este servicio implicaría una contravención a los principios protectores del consumidor.

Por otro lado, se ha cuestionado la responsabilidad del productor si el consumidor no adquiere ningún artículo en el local comercial. Al respecto la Sala mencionada ha dicho que cuando el comerciante ofrece un espacio de parqueo le está ofreciendo al público la posibilidad de que sin llegar a adquirir mercancía determinada dejen su vehículo en el lugar. Con ello, el comerciante adquiere un deber de custodia, guardia y restitución del vehículo. Así, la obligación surge desde el momento en que se ofrece un lugar para estacionar vehículos, independientemente de que sea gratuito, accesorio, complementario, de su actividad principal o de una contraprestación preexistente.

Merece mención particular una sentencia clave para el desarrollo del tema de la Responsabilidad Objetiva, y que enmarca una línea que va a seguir de parámetro para el desarrollo jurisprudencial que le precede. Esta sentencia ha servido como punto de referencia para resolver conflictos con situaciones similares, o por lo menos para ubicar dentro de un mismo plano a cuestiones afines. Se hace referencia a la sentencia del

conocido caso de Monteverde[39], cuyos hechos sucedieron en la sucursal del Banco Nacional de esta localidad, cuando unos sujetos fuertemente armados irrumpieron en el lugar y dispararon contra los usuarios y funcionarios que se encontraban en él.

En esta sentencia se analizan además de la parte penal, la responsabilidad civil de la entidad bancaria por los daños y perjuicios ocasionados por un tercero sin vinculación al banco, pero donde existe un deber de este último de procurar la protección contra los riesgos que puedan afectar la seguridad de los consumidores, según lo estipula el artículo 32 de la Ley de Protección al Consumidor (Ley 7472).

A pesar de que el banco argumentara que los hechos delictivos y los consecuentes daños no le son imputables, por ser un hecho de un tercero, en el fallo se determinó que la acción de un tercero no rompe el nexo causal, pues en el momento en que se crea un Banco se asume la realización de una conducta que si bien lícita, es riesgosa, de tal manera que el daño en el contexto de ese riesgo debe ser asumido por el comerciante. De este modo, se considera que cuando se pone en marcha una actividad peligrosa y esta encaja dentro del régimen de responsabilidad objetiva, porque así se encuentra tipificado y porque coinciden los elementos objetivos y subjetivos, cabe la aplicación de este sistema de imputación.

[39] Sala Tercera de la Corte Suprema de Justicia. Sentencia 01333-2007 de las diez horas con quince minutos del dos de noviembre del dos mil siete.

Para los magistrados, la acción de un tercero no puede desligarse de la actividad del Banco, con el fin de no desnaturalizar el interés de protección del consumidor, quien debe ser protegido, tal y como lo establece la ley, por riesgos contra su salud, seguridad, integridad y por el uso o disfrute de los servicios que se le ofrecen. Este criterio ha sido ya plasmado con anterioridad por la Sala Primera, en el tanto se ha dicho que el hecho de un tercero no exonera al comerciante cuando el riesgo creado es la materialización de dicho hecho[40].

Como en las sentencias anteriormente mencionadas, en la resolución del caso Monteverde también se aclaró que para determinar la posibilidad de dictaminar una posible responsabilidad objetiva, la fórmula a aplicar trasciende más allá del análisis subjetivo o individual, debe verificarse el nexo causal, es decir, que los daños y perjuicios que son producto del ilícito se encuentren enmarcados dentro de la esfera objetiva de una relación de consumo, uso o disfrute de un determinado bien o servicio. Bajo este presupuesto, los magistrados justifican su condenatoria al Banco Nacional por responsabilidad objetiva, ya que el análisis del caso según su punto de vista, desprende que si se suprime hipotéticamente la prestación del servicio el resultado lesivo no se hubiera producido, los daños fueron producidos precisamente en ocasión del servicio

[40] Sala Primera de la Corte Suprema de Justicia. Sentencia 00460-F-2003 de las diez horas cuarenta y cinco minutos del treinta de julio del dos mil tres.

prestado[41], el daño fue producido dentro de la esfera que brinda el servicio de Banca, por lo que no opera la excepción de hecho de un tercero.

En este mismo sentido, se ubica la posición del jurista nacional Dr. Víctor Pérez Vargas, quien en un artículo publicado en el periódico La Nación, mencionó lo siguiente:

> *"De un análisis comparativo de los fallos anteriormente citados se induce la regla jurisprudencial de que el hecho delictivo realizado por un tercero, sin relación alguna con el comerciante demandado, no descarta la responsabilidad civil objetiva de este último por los daños producidos en la persona o bienes del consumidor, en razón de haber ocurrido dentro de la esfera del servicio que se brinda."*[42]

[41] Se citan las resoluciones: Sala Tercera de la Corte Suprema de Justicia. Sentencia 117-2005 de las dieciséis horas con veinticinco minutos del veintinueve de setiembre del dos mil cinco y Sala Primera de la Corte Suprema de Justicia. Sentencia 000295-F-2007 de las diez horas cuarenta y cinco minutos del veintiséis de abril del dos mil siete.

[42] PÉREZ VARGAS, Víctor (2008, 13 de enero). Fraudes Informáticos. Periódico La Nación, Opinión. P. 15.

CAPÍTULO SEGUNDO

Banca por Internet y los Delitos Informáticos

SECCIÓN I

LA BANCA POR INTERNET COMO NUEVO MEDIO PARA REALIZAR TRANSACCIONES BANCARIAS

1.1 EL COMERCIO ELECTRÓNICO

Con el pasar de los años la tecnología ha desarrollado una serie de herramientas de las cuales se sirve el ser humano para facilitar sus labores habituales. El avance en ciencia y técnica ha sido tal que ha puesto al servicio de la humanidad facilidades que no se pensaban como posibles, no hace muchas décadas.

Gracias a los procesos de globalización y la denominada "Era de la información"[43] se han generado radicales cambios en las formas de comercio tradicional que han revolucionado los esquemas establecidos. Ello pues se ha desarrollado una serie de tecnologías que permiten el intercambio de bienes y servicios, así como las más diversas formas de contratación entre partes a través de instrumentos electrónicos, con el fin de llegar a la satisfacción de intereses de una sociedad cada vez más internacionalizada.

El comercio electrónico[44] se convierte en un nuevo medio para realizar transacciones[45], concretar negocios, adquirir bienes y servicios, entre otros, y ha recibido un mayor impulso por medio de la red abierta Internet. Esta red ha funcionado pues resulta un medio ágil, económico, global, y que ha logrado una integración social impensable, de gran eficacia para promocionar el consumo.

[43] Se denomina "era de la información" al momento histórico actual pues se considera que la información es el bien más valioso y motor de la economía.

[44] Comercio Electrónico es conocido también como E commerce, E com, Comercio Virtual, Comercio Digital o En línea y consiste en realizar transacciones por un medio electrónico, principalmente Internet, pero no exclusivamente, pues se incluyen la televisión, el teléfono, el fax, los sistemas electrónicos de pagos y transferencias monetarias, el intercambio electrónico de datos, como instrumentos a través de los cuales se lleva a cabo el comercio electrónico (Según indica la Organización Mundial de Comercio, citada por PORTELA ROJAS María y SOTO MORA, Catalina (2002). *Propuesta de Regulación del Comercio electrónico en Internet (Análisis a la Ley Modelo sobre comercio electrónico de la CNUDMI)*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho. P.P. 10 y 11.)
Es menester aclarar que el presente trabajo enfocará su estudio en el Comercio Electrónico realizado a través de la red Internet, en específico la Banca por Internet, como se verá más adelante.

[45] Este término es entendido en sentido amplio, v.g. producción, entrega, distribución, venta, comercialización de bienes y servicios, publicidad y consumo a través de redes de telecomunicaciones.

El término Comercio Electrónico puede diferenciarse del concepto de Comercio Digital entendiendo el primero como aquel que se realiza a través de cualesquiera medios tecno-electrónicos, mientras que Comercio Digital se entenderá como el que se realiza por medio de redes de computadoras interconectadas (Internet, Extranet, Intranet), por lo que puede decirse que Comercio Digital es la especie siendo Comercio Electrónico el género, en razón de que este último se referirá en general a la utilización de cualquier soporte físico-electrónico para verificar una transferencia de información.[46]

Aproximadamente desde los años 70 se ha dado un tipo de comunicación electrónica de información entre empresas, esto utilizando la tecnología que se conoce como *EDI*, por su nombre en inglés "*Electronic Data Interchange*", que permite transmitir información de una computadora a otra, usualmente estructurándose ésta de acuerdo a normas técnicas específicas.[47] El EDI es una red privada que se utilizaba para realizar comunicaciones comerciales entre empresas. Es cuando aparece el Internet, en su fin comercial, y específicamente con la aparición del *WWW* (*World Wide Web*) que se revolucionó el

[46] LÓPEZ CHAVARRI, José Francisco (2001). Seguridad transaccional en la contratación electrónica privada. Tesis de grado para optar por el título de Licenciado en Derecho Universidad de Costa Rica, Facultad de Derecho. Pp. 9 y 10.
[47] PORTELA ROJAS, María y SOTO MORA, Catalina (2002). Propuesta de Regulación del Comercio electrónico en Internet (Análisis a la Ley Modelo sobre comercio electrónico de la CNUDMI). Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho. Pp. 12

comercio electrónico y se transformó en un fenómeno económico. Así, se crea un sistema de mercado con nuevos participantes, productos y procesos.

En comparación del comercio electrónico tradicional con el comercio electrónico por Internet, se puede indicar que en el primero se trata de una comunicación sólo entre empresas, mientras que con el segundo se involucran empresas y consumidores, empresas y empresas, empresas y administraciones públicas y usuarios con usuarios. Además, con el comercio tradicional los participantes se manejan usualmente en círculos cerrados, con un número limitado de participantes empresariales, mientras que con el comercio electrónico en Internet se da un número ilimitado de participantes, participan tanto conocidos como desconocidos, las redes son abiertas, la red es el mercado; esto provoca que la seguridad y la autenticación se perfilen como necesarias.

Se puede clasificar los distintos tipos de Comercio Electrónico de la siguiente manera[48]

a) Comercio electrónico de Empresa a Empresa (Business to Business).

b) Comercio electrónico entre Empresa a Consumidor (Business to consumer).

[48] Doctrinariamente aparecen diversas clasificaciones, siendo ésta una unión de las más comúnmente adoptadas, sobre el particular no se pretende ahondar pues el presente trabajo indica el Comercio Electrónico como una referencia para abordar el tema de la Banca por Internet, para mayor información sobre el mismo puede recurrirse a los Trabajos Finales de Graduación antes citados de LÓPEZ CHAVARRI, José Francisco (2001). *Seguridad transaccional en la contratación electrónica privada* y PORTELA ROJAS María y SOTO MORA, Catalina (2002). *Propuesta de Regulación del Comercio electrónico en Internet (Análisis a la Ley Modelo sobre comercio electrónico de la CNUDMI)*.

c) Comercio electrónico Empresa a Gobierno (Business to Government).

d) Comercio electrónico persona a persona (Consumer to consumer).

e) Comercio electrónico entre consumidor y empresas (Consumer to Business).

f) Comercio electrónico entre Gobierno y consumidor (Government to consumer).

Quedan así definidos algunos de los actores de este mercado, tales como: las empresas, el consumidor, la Administración Pública; cada uno de ellos con necesidades particulares y características propias en este novedoso medio.

En búsqueda de una legislación unificada y armónica que regule el tema del Comercio Electrónico para solventar necesidades tales como la Seguridad Transaccional, el Derecho del Consumidor y la resolución de conflictos originados como producto de la utilización de este medio se generó en 1996 la Ley Modelo de la CNUDMI (UNCITRAL por sus siglas en inglés) sobre el Comercio Electrónico, elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), que funge como el principal órgano jurídico del Sistema de las Naciones Unidas en la esfera del derecho mercantil internacional.[49]

[49] CNUDMI, "Un mundo de comercio: un derecho mercantil uniforme" disponible en http://www.uncitral.org/spanish/commiss/geninfo-s.htm citado por PORTELA ROJAS María y SOTO MORA, Catalina. op. cit. PP.5O

De esta forma, se manifiesta como un objetivo el que se brinde un marco que permita la interpretación uniforme para los textos legislativos y demás disposiciones que se elaboren con el fin de regular la actividad comercial internacional.

La Ley Modelo fue aprobada luego de varios estudios en periodos de sesiones en 1998 y dentro de sus características se destaca el que deja abierta la posibilidad a las diferentes naciones que la adopten de incorporarla a su derecho de manera tal que no lesione ninguno de sus parámetros legales internos, lo que se ha criticado pues se considera que de utilizarse este recurso en todo el articulado se estaría frenando el propósito de la Ley que es la homogeneización y más bien se estaría creando una separación.[50]

Otro de los objetivos de esta Ley es facilitar el uso de nuevos medios de comunicación y de almacenamiento de información utilizando equivalentes funcionales para los medios tradicionales de comercio, así por ejemplo, implementar el uso de firma digital y certificados digitales para darle validez a negocios jurídicos sin la necesidad de que se manifiesten en su forma escrita. El propósito de lo anterior es eliminar cualquier tipo de traba que pueda surgir en la realización de comercio internacional por la limitación que pueda significar el uso de documentos en papel.

[50] PORTELA ROJAS María y SOTO MORA, Catalina. op. cit. P 57.

Con el propósito de incorporar la Ley Modelo, la CNUMDI emitió una Guía[51] que pretende dejar claros los conceptos y principios de la Ley para que de esta manera sean aplicados adecuadamente en las legislaciones que adopten la Ley Modelo dentro de su sistema jurídico.

El papel que la CNUMDI ha jugado en la elaboración de leyes modelos y recomendaciones ha sido de gran importancia para lograr la uniformidad legislativa, así como facilitar el marco referencial en la elaboración de reglas para facilitar el comercio electrónico.

i. Banca Electrónica

Tal y como indica Sergio Rodríguez Azuero[52], "se utiliza la expresión "electrónica" pues ha sido la más extendida en el lenguaje del sector. En estricto rigor, sin embargo, esta nueva banca se soporta en los importantes desarrollos de la electrónica, incluidos los microcircuitos, con su capacidad lógica de proceso y de almacenamiento de información;

[51] Conocida como Guía para la Incorporación de la Ley Modelo de la CNUMDI sobre Comercio Electrónico, para abreviar se utilizará en adelante la denominación La Guía.

[52] RODRÍGUEZ AZUERO, Sergio (2002). *Contratos Bancarios: su significación en América Latina*. Colombia. Quinta edición. Legis Editores S.A. P. 197.

pero así mismo, en el desarrollo de las comunicaciones que ha permitido construir distintos tipos de redes, y para ellos diferentes protocolos; y desde luego, el desarrollo de la informática, como tal, pues los programas o aplicativos han obtenido niveles que contribuyen con los dos factores anteriores a la transformación global."

Como parte del comercio electrónico y las modificaciones que éste ha traído a las relaciones jurídicas tradicionales, se desarrolla la denominada Banca Electrónica. Por medio de ella, se cambia el paradigma de prestación personal de servicios, a saber: una relación estrictamente personal entre el cliente y su banco, en donde el primero debía acudir a las instalaciones del segundo para realizar sus transacciones bancarias. Así, la concepción de espacio físico, ubicación estratégica en puntos de mercado, empleados capacitados, horarios, días feriados o de descanso, ha ido cambiando con gran rapidez.

> *"La posibilidad de prestar servicios a través de nuevos canales de comunicación entre el banco y la clientela, ha quebrado el paradigma y comienza a eliminar el símbolo. Cada vez la prestación es menos personal y directa. Cada vez se requieren menos oficinas y puntos fijos de atención. Cada vez se desea menos la presencia física de los clientes o los terceros que con ellos contratan en los "halles" bancarios. No se requieren locales, pero tampoco hay que respetar horarios. No hay días feriados ni distancias*

geográficas. La comunicación por distintos medios permite, ante todo, no sólo que se cuente con un soporte de sistemas mucho más eficiente que nunca, para la prestación de estos servicios, sino que los mismos se puedan hacer a distancia y valiéndose de mecanismos que, incluso, comienzan a sugerir como innecesaria la tradicional vinculación entre un cliente y un banquero cualquiera, ante la posibilidad de que aquel pueda obtener a través de los nuevos medios de comunicación, respuestas comerciales, que en un momento o, por lo menos, para algunos servicios, parezca hacerlo inútil."[53]

Así, puede definirse Banca Electrónica como aquella transmisión de datos que permite la comunicación e interacción entre el cliente y el banco a través de impulsos electrónicos, por medio de instrumentos electrónicos y sin que sea necesaria la presencia física de las partes para llevar a cabo las operaciones. También ha sido definida, en una acepción amplia, como todos aquellos elementos de la automatización bancaria que permiten la existencia de una banca plenamente informatizada que pueda denominarse en sentido propio banca electrónica y, por tanto, no sólo incluye la proyección externa de la banca en el mercado a través del ofrecimiento de servicios automatizados, sino además alude a

[53] RODRÍGUEZ AZUERO, Sergio. op.cit. PP. 198 y 199.

segmentos de la automatización bancaria que conciernen al manejo interno del banco y a sus relaciones con otras entidades.[54]

La modernización de la banca latinoamericana siguió el ejemplo de lo ocurrido en los Estados Unidos, en donde en los años 70 se desarrollaron una serie de innovaciones tecnológicas para facilitar la automatización de procesos y la actualización de la información.

> *"A comienzos de la década de los 80, varios bancos y entidades financieras contaban con un gran adelanto en el área de sistemas, que los colocaba en situación semejante a la de los países más desarrollados, logrando un cambio radical en la filosofía de la prestación de servicios en el campo de la transferencia electrónica de fondos y en la modernización de sistemas de pago. Se buscó, por lo tanto, la mejora cualitativa de la prestación de servicios, brindando a los clientes facilidades a través de terminales de autoservicio y cajeros automáticos."*[55]

En términos de costo y beneficio, la opción de Banca Electrónica significa una verdadera ventaja para el sector bancario, pues reduce considerablemente sus gastos al

[54] CIFUENTES, Manuel (2000). *"Una mirada introductoria al mundo de la Banca Electrónica"*. Citado por RODRÍGUEZ AZUERO, Sergio. op. cit. P. 199.
[55] RODRÍGUEZ AZUERO, Sergio. op.cit. P.207.

no tener que invertir en salarios de personal capacitado, instalaciones, recibos por servicios públicos, equipo, entre otros; incluso señala Sergio Rodríguez que en estudios internacionales se ha estimado que mientras una transacción a pie de sucursal le cuesta a la institución bancaria cerca de un dólar, la realizada a través de Internet puede estar alrededor de seis centavos de dólar.

A pesar de lo anterior, no puede pasarse por alto que la utilización de herramientas electrónicas ha provocado el surgimiento de nuevas figuras de fraude, situación que debe ser prevenida y mitigada por los bancos, y por lo tanto requiere una inversión fuerte en el tema de seguridad transaccional, para así evitar el riesgo que se pueda generar. Es de criterio del sector financiero, en especial por los informáticos[56] dedicados a manejar los sistemas electrónicos que brindan en sus entidades, que los costos por mantener sus sistemas seguros son sumamente altos. No obstante, como punto de vista personal, se considera que este costo debe ser sufragado definitivamente, máxime cuando la Banca Electrónica efectivamente se convierte en un beneficio para el Banco, de ahí nace su obligación de mantenerlo como un sistema seguro y así realizar las contingencias necesarias para minimizar los riesgos, que en este medio nunca dejan de existir.

[56] Fue así manifestado en entrevistas realizadas a los Ingenieros Informáticos del Banco Nacional Ing. Cilliam Cuadra (16 de Setiembre de 2009) y del Banco de Costa Rica Ing. Alejandro Sebiani (14 de Setiembre de 2009), con respaldo de grabación de voz.

Continuando con el análisis de la banca electrónica, puede indicarse que la informática y en general la tecnología le han brindado diversas posibilidades a los sistemas de información existentes, que les agregan rapidez, eficacia y comodidad. De esta manera, la banca ha sufrido transformaciones en sus soportes operativos, con el fin de desarrollar nuevas posibilidades para sus clientes; también la prestación del servicio se ha modificado, pues existe una nueva forma de contratar, es decir, pueden realizarse contratos de una manera no típica, por ejemplo, los contratos realizados por Internet.

Esta herramienta ha sido implementada por los bancos en una época en donde competir se ha vuelto indispensable para sobrevivir, ya que se vive en un periodo en donde el consumo y la información son bienes de primer orden, y aquella empresa que no goce de los privilegios de publicidad y tecnología dentro de la "era digital" puede quedar fácilmente obsoleta y perder el insumo básico para su desarrollo en el mercado: los clientes.

Dentro de las posibilidades que la Banca Electrónica le ofrece al cliente están[57]:

- Servicio de Caja: el cliente puede depositar los pagos realizados a su favor y ordenar con cargo a sus fondos, así como pagar deudas que tenga frente a

[57] RODRÍGUEZ AZUERO, Sergio. op. cit. PP.202-206.

terceros. Esta función puede realizarse por ejemplo mediante los denominados ATM (*Automated Teller Machines* por su nombre en inglés) o cajeros automáticos.

- Obtención de crédito: es la posibilidad de conectarse con una central a través de cualquier terminal pública, pero especialmente la posibilidad de conexión directa con su banco, utilizando las claves de identificación (*password, I.D*.).

- Mutuo: se suministra una información básica y de forma sumamente rápida el banco puede autorizar el desembolso de un crédito, abonándoselo al efecto a su cuenta corriente.

- Apertura de crédito: obtención de una línea de crédito, cuando no se exija que el contrato conste por escrito.

- Crédito documentario: posibilidad de intercambiar electrónicamente, a través de Internet y en forma segura, información y documentos propios de una transacción comercial, con el fin de reducir al máximo, y si es posible eliminar el intercambio de documentos físicos, lo que puede traer un evidente beneficio en la agilización de las transacciones y en la reducción de los costos.

Esto a través del denominado "Bolero" (*Bill of lading Electronic register organization*), que brinda esta posibilidad a compañías importadoras y exportadoras, a sus bancos y a las empresas transportadoras marítimas a nivel mundial.

- Servicio de transferencias: el destinatario de pagos puede autorizar al banco para recibir en su cuenta los que realicen terceros o que el cliente autorice al banco para realizar pagos a terceros con débito de su cuenta.

- A futuro se perfila que todas las operaciones bancarias van a poder ser realizadas a través de medios electrónicos, dejando atrás el uso del documento en papel.

ii. Banca a distancia o Home Banking:

La Banca a distancia o *Home Banking* es un tipo de Banca electrónica y consiste en permitirle al cliente acceder a su banco desde fuera, es decir, valerse de la tecnología brindada por las telecomunicaciones para ingresar a la plataforma del banco y así realizar sus transacciones.

Como se mencionó supra, las ventajas de esta modalidad de banca son significativas, lo que ha contribuido a su expansión de forma acelerada. Se perfila como ventaja el no tener que ir hasta una sucursal del banco para realizar una operación, sino que de una manera cómoda, rápida y eficaz pueda adquirirse información financiera y no tener que hacer largas filas y esperar un turno para recibirlas por un funcionario bancario.

Existen varios tipos de Banca a Distancia, entre ellas:

a) Banca a través del teléfono:

Por medio de la cual el cliente se comunica con una central telefónica disponible y suministrando una serie de datos que lo identifican obtiene información sobre sus cuentas y tiene la posibilidad de ordenar cierto tipo de gestiones, por ejemplo, el pago de servicios públicos. Este servicio, a pesar de lo cómodo que puede resultar, contiene una serie de riesgos, como podría ser el desvío de llamadas a un número distinto al de la central bancaria.

Este tipo de banca por teléfono también incluye el ofrecimiento de servicios por parte del banco, por ejemplo, la promoción de tarjetas de crédito. Del mismo modo se adiciona el servicio de recordatorio de pago de deudas.

b) Banca por Internet (*Internet Banking*):

La aparición de la red pública Internet ha hecho que el crecimiento de la Banca Electrónica haya sobrepasado cualquier estimación y que se convierta en el medio de acceso por excelencia del cliente a su banco. A través de esta red, miles y miles de consumidores en todo el mundo se conectan y realizan sus operaciones directamente desde la comodidad de un computador.

Este servicio ha sido prestado por los bancos en Costa Rica desde finales de los 90[58] sufriendo una serie de transformaciones desde entonces hasta ahora. Los bancos se sirven de la Internet para publicitar el servicio de *Internet Banking*, obtener de esta manera clientes y crecer como empresa. Así ha sido manifestado por diversas sentencias, entre ellas la 802-2008 del Tribunal Procesal Contencioso Administrativo y Civil de Hacienda[59].

[58] El Banco Nacional introdujo la Banca por Internet en 1999, el Banco de Costa Rica en el 2002 y el Banco Popular en el 2004 (Tomado de entrevistas realizadas a los ingenieros informáticos de dichos Bancos)
[59] En adelante Tribunal Contencioso Administrativo.

Los bancos crean en la red Internet una serie de páginas que cuya función es permitirle a sus clientes ingresar de manera directa a la plataforma electrónica del banco y de esta manera realizar sus transacciones bancarias. En la sentencias que se han generado en cuanto al tema en cuestión, tanto a nivel del Tribunal Contencioso Administrativo como de la Sala Primera de la Corte Suprema de Justicia, se ha dicho que una vez que el cliente o un tercero accede a la página de la institución financiera es como si ingresara a las paredes del edificio que alberga la institución, sólo que en este caso lo haría de una manera más moderna y cómoda, se hará de forma virtual, desde una computadora.

Existen varios tipos de Banca por Internet, incluyendo dentro de esta modalidad aquellos bancos que ofrecen páginas informativas para sus clientes. Se han generado una gran cantidad de clasificaciones dependiendo del interés que tenga la banca en particular de desarrollar una opción para banca en Internet[60]. En la presente investigación, se va a limitar el estudio de Banca por Internet a la Banca Transaccional, y en específico a la Banca transaccional de personas o personal.[61]

[60]Tomado de entrevista realizada el 16 de Setiembre del 2009 al Ing. Cilliam Cuadra Chavarría, funcionario del área de Seguridad del Banco Nacional, con respaldo en grabación de voz.
[61] Esto pues resulta de especial interés para el desarrollo del tema en cuestión que se realice una mirada a lo que la Banca Transaccional de personas ofrece, para delimitar y abordar el problema teórico planteado.

La Banca de personas o banca personal consiste en la banca especializada en la atención y asesoría de personas físicas[62]. Para ello, se han creado un abanico de posibilidades dependiendo del Banco que la persona quiera elegir, permitiéndole por ejemplo, consultas de estados de cuenta, movimientos, realizar pagos en línea de servicios públicos, pago de servicios municipales, pago de colegiaturas, universidades, cuotas y créditos, transferencias fondos entre cuentas, transferencias a terceros, cargos automáticos, entre otros. Esta opción se promociona como un servicio cómodo, práctico y seguro que busca beneficiar al cliente y facilitarle el acceso a la banca. Este servicio se brinda, en la mayoría de los bancos, las 24 horas del día y durante los 365 días del año.

Por ejemplo, en el Banco Nacional se promociona la opción de BN Internet Personal de la siguiente manera:

> *"¿Quiere descubrir su capacidad para hacer de Internet una gran herramienta? ¿Le gustaría tener información y administrar sus finanzas desde su computadora personal, aun cuando se encuentre fuera del país? El Banco Nacional le ofrece estas opciones y muchas más. BN Internet le permite controlar sus finanzas desde su casa, oficina o café Internet. Es seguro, privado y muy conveniente para personas como usted. Todo lo que necesita*

[62] Banco de Costa Rica (2009) http://www.bancobcr.com/bcr.php?id=2 [Consulta del 23 de noviembre de 2009]

es una conexión de Internet y su tarjeta Servibanca ® para obtener su clave de acceso."[63]

El banco HSBC en Costa Rica, establece en su página de Internet lo siguiente con respecto a su servicio de Banca por Internet (Banca Personal):

"HSBC en Línea le ofrece un avanzado y poderoso sistema de tecnología financiera que lo provee de información las 24 horas de día los 365 días del año, permitiéndole de manera ágil y segura, administrar eficientemente sus fondos, realizar sus transferencias electrónicas y efectuar, mediante una novedosa plataforma, diversas consultas sobre sus cuentas, inversiones, créditos y otros aspectos financieros."[64]

En algunos bancos, la suscripción del servicio se realiza de manera inmediata cuando se obtiene una tarjeta, en cuyo caso se dan dos contratos, uno para la tarjeta en sí y otro para el servicio de Banca por Internet, ambos deben firmarse por el cliente y de esta manera se posibilita el uso de la herramienta. Luego debe ingresarse a la página del banco

[63] Banco Nacional (2009) http://www.bncr.fi.cr/BN/info.asp?c=bcaper&sc=ptram&t=ptinter [Consulta del 23 de noviembre de 2009].
[64] HSBC Costa Rica, Banca por Internet (2009) http://www.hsbc.fi.cr/a/bp/banca_por_internet.asp [Consulta del 23 de noviembre de 2009].

y cambiar la contraseña previamente entregada por el banco, de manera confidencial, para poder activar el servicio.

En otros casos la afiliación se realiza de manera directa del cliente con la página del banco. Así, el cliente ingresa a la página y coloca una serie de datos solicitados por el banco, tales como número de cédula, número de la tarjeta, pin de la tarjeta para cajeros automáticos, código de seguridad y una contraseña que debe elaborar para el sitio de Internet con una longitud determinada y una combinación de caracteres, que incluye números y letras. Además, debe indicar que ha leído y aceptado las condiciones estipuladas en el contrato elaborado para los efectos de *Internet Banking*. Las características de afiliación van a depender de las exigencias que cada banco estipule, siendo las anteriormente explicadas un modelo generalmente aplicado.

De la misma forma en que se definen los servicios y la forma de afiliación a la Banca por Internet, así se establecen los sistemas de seguridad con que va a contar cada sitio, es decir, dependiendo de los parámetros que cada banco destine al respecto. Sobre este tema se hablará con más detalle en la Sección III de este capítulo.

1.2 CONTRATO POR MEDIOS ELECTRÓNICOS

Hasta el momento se ha hecho mención del comercio electrónico y los distintos tipos de actividades que resultan de él, a saber, banca electrónica con sus derivados banca a distancia y banca por Internet. Pero no se ha hecho referencia al tipo de relación existente entre el consumidor de servicios informáticos/electrónicos y la entidad que se los suministra. Para obtener un determinado servicio, debe concurrir la voluntad de las dos partes, quien ofrece el servicio y quien lo utiliza. Nacen de este acuerdo, obligaciones de dar, hacer o no hacer alguna cosa.

Este acuerdo de voluntades tiene que ver con situaciones de carácter patrimonial, o contenido económico. En el tema en cuestión, el contrato va a versar en una prestación de servicios a través de una red abierta (Internet) por medio de la cual una entidad financiera se obliga a brindar el servicio de Banca por Internet y la otra persona (el cliente) tiene la posibilidad de accesar a la plataforma digital del banco para realizar sus transacciones "en línea".[65]

[65]RODRÍGUEZ AZUERO, Sergio. op.cit. P. 252: "Dentro de los contratos por medios electrónicos se encuentra el ***clickwrap agreement***, que es un mecanismo frecuentemente empleado en el comercio electrónico y se define como un contrato para la compra o uso de productos o servicios ofrecidos a través de un vendedor en línea. El comprador que se encuentra en línea, por su parte, acepta los términos del acuerdo haciendo un "click" (generalmente sobre un ícono denominado "acepto")."

Debe aclararse que existe una diferencia entre Contratos por medios electrónicos y Contratos electrónicos propiamente dichos. Los primeros se refieren a aquellos que pueden realizarse por teléfono, televisión interactiva, fax, Internet, entre otros, y se trata de un acuerdo de voluntades puro y simple, no son contratos absolutamente innovadores en esencia; mientras que los segundos varían los principios contractuales clásicos al tener como principal característica el flujo de información haciendo contratos dinámicos, cambiantes.[66]

A los contratos por medios electrónicos también se les denomina contratos virtuales, y son aquellos que se concluyen por e-mail o a través de una "*web-site*" en la red Internet. Estos contratos junto con los "telemáticos" a "distancia" y "digitales" no son más que formas o instrumentos negociables ampliamente difundidos y cuya fortaleza está en la facilidad de poner en contacto compradores y vendedores, ubicados en cualquier parte del mundo, de manera que se logre una competencia acorde con un mercado que hoy es masivo y totalmente globalizado.[67]

El contrato por medios electrónicos funciona como un contrato realizado tradicionalmente, con la particularidad de servirse de mecanismos

[66] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel (2003). *Formas Alternativas de Comercio Internacional: La Contratación electrónica y la seguridad jurídica transaccional*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho. PP. 144.
[67] GUERRERO, María Fernanda citada por RODRÍGUEZ AZUERO, Sergio. op.cit. PP. 250 y 251.

tecnológicos/electrónicos para realizarse. De su perfeccionamiento nacen las obligaciones propias del negocio jurídico. La característica particular de este tipo de contratos no es el contrato en sí, sino la forma en que éste se perfecciona.

El perfeccionamiento mismo del acuerdo de voluntades es muy rápido, resulta fundamental la existencia de una etapa precontractual en la que exista total claridad e información sobre su contenido, no sólo porque ello tiene de relevante frente al negocio que pretende formarse, en particular, sino porque, tales prerrequisitos tienden a evitar que términos globalmente dispuestos por una de las partes, vulneren los derechos de los consumidores.[68]

La CNUDMI (UNCITRAL) ha definido que la expresión "Contratación Electrónica" se ha utilizado para referirse a la formación de contratos por medio de comunicaciones electrónicas o mensajes de datos. Desde este punto de vista, se considera como un método para formar contratos y no como un subconjunto basado en una materia especializada cualquiera. Por eso, no se piensa que los contratos electrónicos sean fundamentalmente diferentes a los contratos basados en papel.[69]

[68] RODRÍGUEZ AZUERO, Sergio. op.cit. P. 251.
[69] UNCITRAL. *"Aspectos Jurídicos del Comercio Electrónico – Contratación Electrónica"* citado por RODRÍGUEZ AZUERO, Sergio. op. cit. 251.

Este tipo de contratación es válida de acuerdo a los principios de autonomía de la voluntad y de libertad contractual, siempre y cuando cumpla con la ley y no quebrante ningún principio estipulado para los contratos en general. En nuestro ordenamiento, no se ve afectada la validez o fuerza obligatoria de un contrato por el hecho de que las declaraciones de voluntad negociales se emitan por medio de datos comunicados entre terminales de computadoras, ya sea por Internet, Extranet o Intranet.[70]

La CNUDMI también ha manifestado que no debe restársele validez a un contrato porque haya sido producido mediante un mensaje de datos, por el contrario, debe procurarse que tenga la misma validez que un contrato escrito o un documento consignado en papel. Lo que le da exactitud al contrato electrónico es su autenticidad, integridad, no repudio y firma digital del documento.[71]

Existe lo que se designa como "consentimiento virtual" y tiene que ver con la expresión de la aceptación ante una oferta hecha por la Internet, en donde lo único que varía es el medio por el cual se lleva a cabo.[72] El consentimiento es un fenómeno bilateral, en el que se expresan dos voluntades. Sin embargo, en algunos contratos, los adhesivos por ejemplo, la palabra consentimiento sería mal utilizada, pues no existe realmente un acuerdo mutuo de voluntades, sino que una de las partes decide adherirse a los términos

[70] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel. Op. cit. P 151.
[71] Sobre estos conceptos se volverá con detalle en la sección III de este capítulo.
[72] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel. Op. cit. P. 156.

previamente impuestos por uno de los sujetos del contrato, de manera tal que existe una declaración única de voluntad. Entonces, bajo el concepto de "consentimiento virtual" debe entenderse un acuerdo mutuo de voluntades, un consenso, al que han llegados dos o más partes a través de medios electrónicos.

En la doctrina, el consentimiento se trata de explicar con tres puntos fundamentales[73]:

a) "*On-line*": en tiempo real, caso en el cual la doctrina discute si se está ante un contrato entre ausentes o entre presentes, pero que en todo caso, si se admite que es entre presentes será una "presencia virtual" y siempre bajo las características de un contrato a distancia.

b) Por medio de un correo electrónico, "e-mail" o mensajería electrónica.

c) Aceptación de la oferta mediante un "click" del Mouse. Corresponderá preguntarse si se está frente a la expresión de un asentimiento o no.

Los elementos de forma para los contratos tradicionales deben mantenerse para los realizados por medios electrónicos, exceptuando por supuesto la elaboración escrita del

[73] Ibídem. P. 160.

documento, pues se equipara la validez del documento digital con el papel. Debe guardarse una constancia escrita del contrato para que sea accesible para su posterior consulta. El contrato por medio electrónico, al igual que todos los contratos, debe manifestar la existencia de un acuerdo de voluntades inequívoco sobre el objeto del contrato, además no debe presentar vicios que lo deje sin efectos.

En general se sostiene que las presentaciones a través de medios electrónicos no pueden ser consideradas estrictamente como ofertas. La oferta estaría constituida propiamente por quien responde a la invitación u "oferta especial de una página electrónica"[74] La CNUDMI ha establecido que la aceptación de la oferta es efectiva en el momento en que exista asentimiento del destinatario, y que tendrá efecto en el momento en que la indicación del asentimiento llegue al oferente.[75]

[74] RODRÍGUEZ AZUERO, Sergio. op.cit. P. 254.
[75] Convención Internacional de Mercaderías y Operaciones Conexas de UNCITRAL. Artículo 18. Citado por RODRÍGUEZ AZUERO, Sergio. op. cit. P.255

SECCIÓN II

ALGUNOS DE LOS DELITOS INFORMÁTICOS QUE MÁS HAN PERJUDICADO A LOS CLIENTES DE BANCA POR INTERNET

Dentro de los delitos que más han afectado a los usuarios de Banca por Internet se encuentran los denominados fraudes por robo de identidad[76], a continuación se detallan los que han tenido más incidencia en la población consumidora de servicios bancarios por Internet.

[76] Robo de identidad se puede utilizar para describir el robo o la asunción de una identidad existente (o una parte significativa de la misma), con o sin el consentimiento de la persona, y con independencia de si ésta está viva o muerta. PAGET, François (2007).*Robos de Identidad*. Mc Afee Avert Labs. www.mcafee.com [visitado el 02 de Octubre de 2009].

2.1 EL DELITO DE PHISHING: MATRIMONIO ENTRE LA TECNOLOGÍA Y LA INGENIERÍA SOCIAL[77]

Se pueden encontrar varias definiciones para el término *Phishing*, esto se debe principalmente a que se encuentra de forma constante en evolución. Así las cosas, se considera como *Phishing* la acción fraudulenta a través de la cual se procura conseguir información confidencial, como el número de tarjeta de crédito o la contraseña de las cuentas bancarias, ya sea mediante la imitación de un correo electrónico de una institución financiera legítima o mediante técnicas un poco más avanzadas que logran que los usuarios ingresen a páginas electrónicas en apariencia iguales a las del banco y desde las mismas revelen sus datos personales.

El término *Phishing* proviene del vocablo en inglés *fishing* cuyo significado en nuestra lengua sería "pescando", esto porque se considera que los responsables de este tipo de actividad se encuentran pescando información personal; por su parte el *ph* se deriva de

[77] El término Ingeniería Social ha sido utilizado con diversas acepciones, en esta investigación será utilizado con relación a los delitos informáticos, ya que este concepto fue usado y popularizado inicialmente con un sentido muy distinto por la jurisprudencia sociológica norteamericana. El Profesor de Harvard Roscoe Pound, por ejemplo, considera al Derecho como ingeniería social. Para Pound, el Derecho es ingeniería social: organiza y reconstruye la sociedad en base a sus necesidades. No se plantea cuestiones de Justicia, sino si el sistema aplicado es práctico. POUND, Roscue (1954). *El Derecho como Ingeniería Social*. Edición Losada. Buenos Aires, Argentina.

las sofisticadas técnicas que se utilizan como anzuelo para de esta forma distinguir o separar esta actividad de una simple pesca (*fishing*).[78]

Los ataques denominados *Phishing* usan mensajes de correo engañosos y servidores fraudulentos con la intención de engañar a los usuarios de servicios de Internet. En el caso de las entidades financieras, el objetivo es intentar que los usuarios divulguen sus datos, como el número de tarjeta de crédito o sus claves de acceso PIN.[79]

Cuando se hace referencia al *Phishing* se debe de considerar la estrecha relación que existe con el concepto de ingeniería social. A pesar de que se observa que los ataques atribuidos a técnicas de *Phishing* pueden ser efectivos sin importar si estos utilizan o no la ingeniería social, es muy común que la tasa de efectividad de estos ataques se vea incrementada cuando el atacante utiliza ambos componentes de una manera estratégica. Es por esta razón que a la hora de referirse al *Phishing* se debe de estar familiarizado con el concepto de ingeniería social.

[78] Traducción moderada de LANCE, J. Y STEWART J (2005). *Phishing exposed, uncover secrets from the dark side*. Syngress Publishing, Inc. P. 2

[79] Banco de Costa Rica (2009) http://www.bancobcr.com/bcr.php?id=121 [Consulta del 23 de marzo de 2009].

En términos generales se puede considerar que la ingeniería social se refiere a la manipulación de las personas para que voluntariamente realicen actos que por lo general no harían[80].

Enfocando este concepto hacia un punto de vista relacionado con la seguridad de los sistemas informáticos, se puede entender la ingeniería social como el término usado entre crackers para referirse a las técnicas de violación que se sustentan en las debilidades de las personas más que en el software. El objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad del sistema objetivo[81].

En términos de los empleados bancarios especialistas en este tema, el objetivo de los crackers es atacar al "eslabón débil" de la relación, a través del engaño y la manipulación para que entreguen sus contraseñas y de esta manera se ingrese a la página del banco suplantando la identidad del cliente, actuando como si fuera éste y dañando su patrimonio.

[80] BISCIONE, Carlos. *Ingeniería social para no creyentes.* <http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf>. [Consulta: 24 marzo. 2009].
[81] Traducción moderada de *The complete social engineering faq!*. <http://packetstorm.linuxsecurity.com/docs/social-engineering/socialen.txt>. [Consulta: 25 marzo. 2009].

También se da la creación de páginas de Internet falsas, que es un fenómeno conocido como *web spoofing*[82], ello con el fin de que los clientes bancarios ingresen a éstas y suministren sus datos confidenciales para realizar la estafa.

El *Phishing* ha sido definido por expertos en el tema de tecnologías de seguridad de la siguiente manera:

> *"El Phishing generalmente es un correo electrónico que le envían a las personas en apariencia con un mensaje con una alerta máxima de algo que está pasando en el banco, que tiene que ver con modificación de datos, ingreso a las cuentas, o con cancelación de cuentas, un mensaje alarmista que asuste a la persona y que la haga ingresar a una página con apariencia similar a la del banco, por lo menos en colores tal vez pero no en las técnicas y usos, es una técnica muy efectiva, es un fraude muy sencillo por engaño; con un engaño muy sencillo y muy trivial la gente da sus datos y con ello obtienen la identidad necesaria para hacer un fraude. En Phishing envían el correo a cuentas que son aleatorias, ellos toman un listado de cuentas con apellidos comunes en Costa Rica como Alfaro, Rojas, Jiménez, empiezan a enviar todas las combinaciones, empiezan con los nombres más comunes en Costa Rica como María, Carmen, y*

[82] FERNÁNDEZ, Rosa (2006). *Reseña de la Jornada sobre los riesgos penales de la banca on-line*. http://www.uoc.edu/idp/2/dt/esp/fernandez.pdf. [Consultada el 25 de noviembre de 2009]

empiezan a unirlos con Jiménez, Rojas, etc. para llegar a las cuentas. Para ellos tiene un costo importante de alrededor de $3 000 pero están dentro de la idea que pueden mandar todos los mensajes que sean necesarios, incluso si el correo al que envían no existe, en general para el atacante es igual mandar 1 000 que 3 000, siempre va a ser el mismo costo y por lo tanto la gente a veces se cuestiona porqué ellos sabían mi cuenta de correo, realmente ellos no sabían su cuenta de correo, lo mismo sucede con su cuenta bancaria, ellos realmente no sabían si usted tenía o no cuenta en el banco, es pura prueba y error, es cuestión de probabilidades."[83]

"Phishing es bastante simple, envía un correo electrónico aparentando ser el banco, que eso es muy fácil de hacer, entonces se enmascaran como si fueran un banco real, e invitan al cliente a que ingrese a su sitio ya sea bajo amenaza o bajo motivación. Por ejemplo, si usted no ingresa su cuenta será cerrada, entonces mucha gente reacciona de esa forma a la presión, Cuando es bajo motivación lo que se hace, por ejemplo, es decir que se está haciendo una rifa de un crucero por Alaska, que participe, entonces se lleva de estas formas, ya sea por presión o motivado, a sitios falsos donde le pedían usuario y clave."[84]

[83] CUADRA CHAVARRÍA, Cilliam. Ingeniero informático Banco Nacional. Tomado de entrevista realizada el 16 de setiembre del 2009.
[84] SEBIANI SERRANO, Alejandro. Ingeniero Informático Banco de Costa Rica. Tomado de entrevista realizada el 14 de setiembre de 2009.

Este delito informático es uno de los que más ha afectado a los usuarios de Banca por Internet, las explicaciones al respecto son variadas, dependiendo sobre todo de la línea que se quiera seguir, es decir, en la tesis bancaria, se argumenta que el cliente es quien ha tenido la responsabilidad por su descuido e "ingenuidad"[85] en Internet, mientras que del lado del consumidor se ha expresado principalmente una falta de información (incluso se ha dicho que la información proporcionada no era concordante con la realidad) omitiendo hacer de conocimiento del usuario el riesgo que la actividad conlleva. Así las cosas, mayoritariamente ha sido aceptado por el Tribunal Contencioso Administrativo y por la Sala Primera que ha existido una responsabilidad de los bancos en el tanto no contaban con las medidas de seguridad necesarias para prestar un servicio que se cataloga como riesgoso[86].

Algunas recomendaciones[87] para evitar el *Phishing* son, por ejemplo, el recordar que la banca nunca solicita información personal o financiera por ningún medio, es decir, no se deben enviar datos personales o brindarlos de ninguna manera a correos electrónicos o llamadas telefónicas. Adicionalmente, cuando se hace conexión con los servicios de *Internet Banking* se debe comprobar que la navegación es segura (fijarse en el candado de

[85] Este término, considerado peyorativo a criterio personal, fue escuchando en varias de las entrevistas realizadas durante la recopilación de información para la presente investigación.
[86] Sobre este particular se abordará más adelante en detalle.
[87] Estas recomendaciones pueden ser encontradas también en las páginas de Internet de los bancos, como información de seguridad para el cliente, también en "demos" y guías virtuales.

seguridad localizado en la esquina inferior derecha de la pantalla, digitar la dirección directamente en el navegador y no hacer clic en las que aparecen en correos o buscadores, verificar el certificado de seguridad, entre otros) además que el sitio web bancario transmite su información encriptada por medio del protocolo SSL (Secure Sockets Layer)[88] que se identifica al aparecer https en la dirección. Esto garantiza la comunicación entre el servidor y el cliente y la autenticidad del servidor al que se conecta; además evita que otros capturen o vean los datos intercambiados y que el servidor sea suplantado por un tercero.[89]

Una prueba rápida para comprobar la veracidad del sitio en Internet del banco es tal y no ser engañados por webs creadas para robar datos, es dar un "doble clic" sobre el candado amarillo que aparece en la parte inferior derecha del navegador, una vez realizado esto, saldrá el certificado de autenticidad que asegura la identidad del banco.[90]

[88] Sobre estas recomendaciones así como la Seguridad Transaccional se estudiará con detalle en la Sección III de este capítulo.
[89] FERNÁNDEZ LÁZARO, Fernando (2007). *"Los nuevos medios de investigación en el proceso penal: especial referencia a la tecnovigilancia. Medios técnicos en la Investigación de los Delitos Informáticos*". Madrid, España. Primera edición. Consejo General del Poder Judicial. PP. 191 Y 192
[90] Ibídem.

2.2 EL PHARMING

El *Pharming* es otra de las modalidades delictivas que también han afectado en gran medida a los usuarios de banca por Internet. Este fraude informático utiliza métodos más elaborados que el *Phishing*, es por ello que se ha desarrollado como el siguiente paso para defraudar a los clientes en el momento en el que el *Phishing* pierde fuerza por el conocimiento de la población de los casos relacionados con éste.

El *Pharming* es una práctica delictiva en la que un pirata informático desvía el tráfico de Internet de un sitio *web* hacia otro de apariencia similar, con la finalidad de engañar a los usuarios, para obtener sus nombres y contraseñas de acceso, que se registrarán en la base de datos del sitio falso. Esto se hace con el fin de robar los datos de autenticación y cometer estafas suplantando la identidad de los usuarios.[91]

El desvío del tráfico de un sitio *web* a otro fraudulento se lleva a cabo mediante la modificación en los DNS (Servidor de Nombres de Dominio, por sus siglas en inglés) de los

[91] Ibídem. PP. 192 y 193.

datos que asocian la página verdadera con su dirección IP (Protocolo de Internet)[92], lo que hace que el usuario crea que ha accedido a la *web* verdadera.[93]

El proceso de *Pharming* se hace mediante el denominado "envenenamiento de DNS", en el que el atacante tiene acceso a alguna de las enormes bases de datos que utilizan los proveedores de Internet para enrutar el tráfico web y realiza modificaciones para desviar a los usuarios hacia el sitio falso antes de que éstos tengan acceso a la página deseada.[94]

Explicado en términos de los expertos, el *Pharming* es cuando *"un virus tipo troyano se instala en su equipo, modifica un archivo que los que estamos en el tema de tecnología sabemos que existe y es fácil de modificar, entonces modifica ese archivo y lo redirecciona. Estos virus se aprovechan que usted es el administrador, puede modificar la configuración de su equipo, puede instalar lo que sea y entonces lo hace. Es una modalidad utilizada para engañar al cliente, porque básicamente es un engaño lo que se les hace."*[95]

"Mayor peligro y eficacia encierra la nueva amenaza conocida como

[92] Conjunto de cuatro números del cero al doscientos cincuenta y cinco separados por un punto que van a identificar de manera inequívoca a un ordenador o conjunto de ordenadores que se encuentra conectado a Internet (por ejemplo 255.255.255.255). En el mundo digital, sin embargo, todo funciona con información binaria, por lo tanto los componentes de la dirección IP es un número binario de ocho dígitos, ocho bits (11100111) lo que ofrece un total de dos elevado a ocho combinaciones. Ibídem. P. 128.
[93] Ibídem. P. 193.
[94] Ibídem.
[95] SEBIANI SERRANO, Alejandro. Ingeniero Informático Banco de Costa Rica. Tomado de entrevista realizada el 14 de setiembre de 2009.

Pharming, cuya base de actuación la constituye la alteración de las direcciones DNS, que permiten conducir al usuario, de nuevo, a una página web falsa y no a la que ha solicitado realmente al teclear la dirección. El sistema de ataque puede ser general, si el objeto de asalto son los servidores DNS, en cuyo caso, cualquier usuario que pretenda acceder a la entidad bancaria, cuyo DNS se haya modificado fraudulentamente, en realidad acabará en la página web falsa creada para la recogida de sus credenciales bancarias."[96]

"El Pharming se trata de una sofisticada forma de Phishing que redirecciona la conexión entre la dirección IP y el servidor destino. Esto puede llevarse a cabo en el servidor DNS (a través del envenenamiento de caché o ingeniería social) o en el equipo local con la ayuda de un troyano que modifica el archivo hosts. El vínculo se altera de manera que cada vez que los usuarios intentan conectarse al sitio real de una organización son redirigidos de forma secreta a un sitio de réplica, sin haber introducido en ningún momento la dirección incorrecta (fraudulenta). El uso de ingeniería social es especialmente

[96] FERNÁNDEZ, Rosa. Op. cit. P.2

retorcido, ya que las propias víctimas terminan realizando acciones que les perjudican (…)"[97]

Para evitar ser víctima del *Pharming*, se recomienda no abrir correos electrónicos de direcciones desconocidas, tener un antivirus actualizado, preferiblemente contar con un Anti-Malware, que funciona como un antivirus pero con mayores aplicaciones y por lo tanto va a detectar la presencia de virus, troyanos, gusanos y toda una serie de infecciones que pueden instalarse en el computador y provocar cambios en el Sistema Operativo.

2.3 EL MALWARE

Malware se refiere a una palabra genérica para describir cualquier tipo de programa o archivo dañino para el ordenador. Proviene de una agrupación de las palabras malicious software. Los tipos de Malware más conocidos son los virus, gusanos, troyanos, puertas traseras, *exploits*, programas espías, ente otros[98].

[97] PAGET François (2007).*Robos de Identidad*. Mc Afee Avert Labs. www.mcafee.com [visitado el 02 de Octubre de 2009]. P.7
[98] FERNÁNDEZ, Fernando. op. cit. P. 184

"Son códigos que lo que hacen es leer el teclado o referenciar y buscar dentro de los archivos los passwords y demás cosas que la gente tiene guardada en su computadora, por eso no debe activarse la opción de recordar contraseña, con el malware se buscan esos archivos dentro del sistema operativo para extraerlos. Generalmente se instala por medio de virus o de descargas de archivos, en correos o redes sociales, también por el Messenger."[99]

2.4 LOS VIRUS INFORMÁTICOS

Un virus informático es un programa informático que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse. Los virus se activan cuando se ejecuta el programa o archivo que lo contiene, ejecutando al mismo tiempo el código del virus. Esto provoca los efectos o daños para los que estaba diseñado el virus.[100]

Los virus se encargan de destruir información que se tiene almacenada en la computadora. Los daños que producen los virus pueden afectar los programas (Software) o las máquinas (hardware). Dependiendo del tipo de virus así será el daño que sea capaz

[99] CUADRA CHAVARRÍA, Cilliam. Ingeniero informático Banco Nacional. Tomado de entrevista realizada el 16 de setiembre del 2009
[100] FERNÁNDEZ, Fernando. Op. cit. P. 184.

de provocar, además de eso dependerá también su detección, pues al tratarse de un tema que cambia de manera sumamente veloz, es muy probable que para algunos virus no se haya desarrollado la vacuna o antivirus que lo elimine.

Los virus se reproducen a partir de la existencia de un código "padre", encargado de iniciar la epidemia vírica. Cada uno de los segmentos de los virus son capaces de reproducirse infinidad de veces en soportes magnéticos.[101]

Cuando una computadora está infectada con virus e intercambia información con otras, es muy probable que infecte a esas otras computadoras, en el tanto estas no tengas el antivirus que combata ese virus. Una vez que el virus está activado, puede reproducirse copiándose en discos duros, en programas, en discos compactos, en ficheros que se envían a través de Internet, correos electrónicos, etc.[102]

Los virus también pueden residir en las partes del disco duro que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que se ejecutan automáticamente.[103]

Existen varios síntomas para detectar si un equipo se encuentra infectado con virus,

[101] CHINCHILLA SANDÍ, CARLOS. op. cit. P. 47.
[102] FERNÁNDEZ, Fernando. op. cit. P. 184.
[103] Ibídem. P. 185.

por ejemplo el que se vuelvan más lentos para procesar información, algún tipo de mensaje de burla, y lo más dañino, la pérdida de la información e incluso inutilización del sistema de manera parcial o total. Por ello, es importante obtener antivirus actualizados, de buena calidad y adecuado posicionamiento en evaluaciones internacionales, con el fin de eliminar y prevenir cualquier infección por virus.

Los sistemas de antivirus son programas especialmente diseñados para detectar, identificar y eliminar o inutilizar los virus. Para ello, las empresas de antivirus están constantemente trabajando en la búsqueda y documentación de cada nuevo virus que aparece. Muchas de estas empresas actualizan sus bases de datos todos los días. Por lo tanto, lo realmente importante en un programa antivirus es que el usuario lo mantenga actualizado.[104]

2.5 EL SPYWARE

El Spyware es todo aquel software que recolecta y envía información a los usuarios. Normalmente, trabajan y contaminan sistemas como lo hacen los caballos de Troya (Troyanos). Puede venir asociado a utilidades (reproductor mp3 o un juego) y, generalmente, se ofrece como una clase de software sin cargo (gratuito). El problema es

[104] Ibídem.

que tiene, también, un segundo componente oculto, que recolecta información sobre los hábitos informáticos de los usuarios y envía la información por Internet al creador del software. El hecho que esta actividad suceda sin el conocimiento del usuario, hace que se les denomine "programas espías".[105]

En un inicio, los Spyware fueron utilizados para rastrear los datos que la persona iba generando en Internet con fines de marketing, como por ejemplo, las tendencias de compra de productos o las preferencias que mostraba. Sin embargo, posteriormente se ha utilizado con fines delictivos.

El cuidado que debe tenerse para evitar la instalación de Spyware es descargar aplicaciones únicamente en sitios seguros, fiables y no aceptar cualquier tipo de invitación para abrir y descargar en el equipo un archivo.

2.6 LOS CABALLOS DE TROYA O TROYANOS

Un programa denominado Caballo de Troya o Troyano es un software dañino disfrazado de software legítimo. Así, el programa parece ser inofensivo, sin embargo, de manera oculta contiene una sección de código oculto, que al ser procesado se activa y

[105] Ibídem. P. 187.

provoca graves distorsiones en los sistemas informáticos[106].

El caballo de Troya es un método de manipulación en el procesamiento de datos ingresados[107], y su nombre se deriva de la obra La Ilíada de Homero. Los caballos de Troya no son capaces de replicarse por sí mismos y, por lo tanto, son adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño[108].

Los troyanos son utilizados generalmente para espiar personas, para ello, instalan un programa de acceso remoto que permite monitorear lo que está haciendo, en cada momento el usuario, por ejemplo, la captura de pulsaciones del teclado, las contraseñas, la recepción de capturas de pantalla (muestran lo que el usuario ve)[109].

La mejor manera de protegerse contra los troyanos es, en primer lugar, utilizar un anti-malware actualizado, que como se comentó supra, consiste en un sistema que brinda mayor protección que los antivirus pues detectan todo tipo de amenaza, incluidos los caballos de Troya. Además, no abrir, descargar o ejecutar nada de lo que se desconozca su origen.

[106] CHINCHILLA SANDÍ, Carlos. op. cit. P. 42.
[107] Ibídem. P. 41
[108] FERNÁNDEZ, Fernando. op. cit. P. 186 y 187.
[109] Ibídem, P. 187.

2.7 KEY-LOGGERS

Los denominados Key-Loggers o "registros de tecleo" son programas (malware) que están diseñados para instalarse en la computadora y capturar cada una de las pulsaciones que se hacen en el teclado de la computadora, recolectando así todas las contraseñas que son utilizadas para ingresar, por ejemplo, a un sitio bancario. Busca sólo parejas de usuario y contraseña, para luego enviarlas a otra computadora sin el conocimiento ni autorización del usuario. Es un tipo particular de software espía o Spyware[110].

Con respecto a su funcionamiento, se ha manifestado lo siguiente:

> *"Hay dos tipos de Key-loggers, los físicos y el software .Lo que hacen es que descargan una aplicación (en el caso de los software) o le ponen un aparato a su computadora (el físico), que es capaz de leer cada tecla que escribe, hacen una búsqueda en el código que se genera de esta escritura y encuentran el acceso a las páginas de los bancos y las claves que se utilizó, son lectores de las teclas."*[111]

[110] Ibídem. P. 194.
[111] CUADRA CHAVARRÍA, Cilliam. Ingeniero informático Banco Nacional. Tomado de entrevista realizada el 16 de setiembre del 2009

SECCIÓN III

LO QUE DEBE SER Y LO QUE ES: MEDIDAS DE SEGURIDAD PARA LA BANCA POR INTERNET.

3.1 MEDIDAS DE SEGURIDAD, LO QUE DEBE SER

En esta sección se hará énfasis en el estudio de los distintos métodos aplicables a la Banca por Internet, y en algunos casos al Comercio Electrónico en general, para dotarlo de la seguridad necesaria y que así se ajuste al adecuando cumplimiento del servicio para el que está estructurado.

Alrededor de la utilización del comercio electrónico, existe cierto temor por su característica de impersonalidad, sobre todo en cuanto al consumidor, pues de no regularse adecuadamente velando por su protección, podría encontrarse con gran facilidad en una posición de desigualdad.

Es vital que el consumidor sienta confianza a la hora de realizar sus transacciones

electrónicas, dado que de otra manera, a pesar de las bondades que puede implicar la utilización de medios electrónicos para facilitar el comercio, el público no le daría la aceptación necesaria y por lo tanto, no provocaría los resultados que se espera produzca, tales como agilidad, rapidez, facilidad, comodidad, entre otras.

En el caso del Internet, el cambio es una constante, de ahí que lo que puede considerarse seguro un día, al día siguiente ya no lo es. Los métodos delictivos son cada vez más elaborados y existe un gran interés en vulnerar los sistemas de seguridad de los agentes dedicados al comercio y prestación de servicios por Internet, sobre todo por las grandes cantidades de dinero que se manejan y por las ventajas que el delincuente tiene en la red.

Por ello, es sumamente difícil que con la rapidez que se requiere el Derecho se adecue a las situaciones fácticas tan velozmente cambiantes. Sin embargo, en amparo del consumidor y de la seguridad jurídica que toda relación debe tener, máxime cuando se trata de un nuevo medio para contratar y realizar negocios jurídicos, el Derecho debe hacer uso de sus posibilidades y reglar de forma eficiente y actual para solucionar los conflictos indicando las líneas por las cuales debe dirigirse tal actividad.

Es aquí donde comienza su labor de fundirse con ramas que tradicionalmente se

mantenían separadas, pero que el avance tecnológico ha unido como resultado de una sociedad globalizada y moderna. El Derecho debe proveer alternativas en concordancia con los conocimientos de la Informática para bienestar de los actores comerciales.

Es de conocimiento general, que la promulgación de una ley lleva un procedimiento largo, lleno de modificaciones y de pasos que deben cumplirse, esto en muchos casos se traduce en años y el producto final puede distar en gran medida de la propuesta inicial. Esto representa un gran problema en el tema de seguridad de la Banca por Internet, pues una ley puede carecer de la agilidad necesaria para afrontar los problemas del día a día, que como se mencionó anteriormente, se transforman en minutos, teniéndose en cuenta, además, que los problemas ya se han dado y la solución se solicita ya.

Se tiene como opción, en primer término, crear una ley suficientemente amplia que abarque situaciones generales y encajen presupuestos a futuro. Por ejemplo, la ya mencionada Ley Modelo de la CNUDMI (UNCITRAL) propone alternativas amplias en búsqueda de una unificación normativa para la solución de conflictos a nivel internacional. Una propuesta de este tipo es bastante provechosa para aplicarla en nuestro sistema jurídico, y en varios de sus alcances ya se ha hecho. Sin embargo, no es objetivo de esta investigación proponer una ley, bajo el argumento ya esgrimido de su lenta aprobación.

Como segunda opción, puede hacerse uso de las otras posibilidades que brinda el Derecho y utilizar lo que está ya a la mano. Eso es básicamente lo que ha sucedido en este tema, pues tanto el Tribunal Contencioso Administrativo como la Sala Primera, han resuelto los problemas que se han generado en el tema en estudio con la normativa que existe actualmente. Como se indicó el la Sección I de este capítulo, en el punto 1.2, los contratos por medios electrónicos no vienen a generar un contrato distinto del tradicionalmente dado, únicamente se forma en un medio distinto a éste, justamente a través de medios electrónicos, por ejemplo Internet. De ahí que los presupuestos fácticos de los problemas actuales encajan dentro de lo ya elaborado para los Contratos y sobretodo en la Ley 7472.

Teniendo esto claro, es importante indicar que otra de las alternativas para enmarcar la seguridad dentro de lo que "debe ser" es utilizar la posibilidad de los órganos que regulan la actividad bancaria. De este modo, a criterio personal, se considera que la SUGEF (Superintendencia General de Entidades Financieras) tiene la competencia suficiente para realizar una especie de reglamento o normativas a seguir indicando la seguridad mínima con la que debe contar una entidad bancaria que desee prestar servicios de Banca por Internet, definiendo las pautas mínimas tanto en seguridad de sus sistemas como la que debe brindarle al cliente.

Lo anterior se apunta así pues en dentro de las funciones de la SUGEF se encuentran:

> *"Dictar las normas generales que sean necesarias para el establecimiento de prácticas bancarias sanas.*
> *Dictar las normas generales y directrices que estime necesarias para promover la estabilidad, solvencia y transparencia de las operaciones de las entidades fiscalizadas. "*[112]

Así las cosas, se llegaría a una solución rápida y vinculante para todos las entidades que deseen brindar el servicio de Banca por Internet, teniendo así que cumplir con una serie de parámetros mínimos para poder hacerlo. Debe entenderse como un mínimo de normas, permitiéndose ir más allá e invertir en mayor seguridad si se desea, máxime si se está velando por la mayor protección de los consumidores.

Algunos personeros de los bancos han estado de acuerdo con esta opción, e incluso les parece beneficioso tanto para el consumidor como para los bancos, pues tendrían las reglas claras y en caso de controversia se podría validar el uso de

[112] Superintendencia General de Entidades Financieras (SUGEF).(2009). http://www.sugef.fi.cr/pagina.asp?lang=0&pagina=servicios/documentos/infgeneral/funciones/SUGEF.pdf [consultada el 27 de noviembre de 2009]

herramientas de seguridad de acuerdo a los parámetros establecidos por parte de los bancos.

> *"Sí debería para mí existir una guía básica, indicando lo mínimo que el Banco debería tener, si tiene más excelente, pero lo mínimo debería ser esto. En el caso de los bancos como somos regulados por CONASSIF y SUGEF deberían ser ellos los que la emitan, digamos que ese es el mecanismo más rápido de hacerlo, cuando se trata de hacerlo a nivel de ley la historia es otra, puede tardar años en discusión, entonces esa puede ser una forma más rápida de hacerlo."*[113]

Por otro lado, existe la posición de que cada banco debe mantener su seguridad según el sistema de banca por Internet que quiera prestar, que cada uno debe encargarse de incorporar las medidas de seguridad que crea necesarias. Así, confían más en la opción de una autorregulación antes que una regulación establecida por un ente superior. Esta posición no se comparte, en el tanto para brindar seguridad jurídica, tanto al consumidor como al banco, debe establecerse un mínimo de medidas con las que por obligación toda entidad que quiera asumir la prestación del servicio deba necesariamente cumplir.

[113] SEBIANI SERRANO, Alejandro (2009). Ingeniero Informático Banco de Costa Rica. Tomado de entrevista realizada en San José el 14 de setiembre de 2009.

Volviendo en el punto de la confianza y la seguridad que las transacciones por Internet deben asegurarle al usuario, se considera que Internet es "inherentemente inseguro"[114], presenta riesgos que siempre estarán presentes, al ser una red abierta, se encuentra disponible para personas con variedad de intenciones, algunas veces no las mejores, es tan grande el volumen de las transacciones que viajan por Internet, que toda transferencia de datos puede ser potencialmente leída o monitoreada por un tercero.

> *"Estos riesgos pueden ocurrir tanto en un ambiente legítimo para gerenciar el trabajo en red, como en uno ilegal para actividades como el robo de los números o claves de las tarjetas de crédito."*[115]

La seguridad de la información ha sido definida como aquellos pasos preventivos que se toman para proteger tanto la información como las capacidades. Se pretende proteger estos elementos de las amenazas y que alguien pueda explotar alguna vulnerabilidad[116].

[114] MARCUCHI, Jackeline citada por RODRÍGUEZ AZUERO, Sergio. op. cit. P. 241.
[115] Ibídem.
[116] MAIWALD, Eric (2005). *Fundamentos de Seguridad de Redes*. México. Segunda Edición. Mc Graw-Hill Interamericana Editores, S.A. P. 4

La seguridad en las transacciones se ha convertido en una exigencia en el comercio electrónico. La doctrina ha señalado cuatro elementos fundamentales para que las comunicaciones vía informática sean seguras[117]:

a) La Autenticidad:

Hace referencia a la veracidad de las partes que intervienen en una relación, con su identificación en la red Internet. Cuando se ingresa a una página y se contacta con un comerciante, se asume el riesgo que la persona o entidad no sea quien dice ser. Por ello, se hace necesario el tener seguridad sobre quién es efectivamente la persona con la que se está transando.

b) Confidencialidad o Privacidad:

Al ser Internet una red pública, y manejar cientos de información, aunado a que cada cosa que se hace en ella deja una "huella tecnológica"[118] existe una gran probabilidad que las comunicaciones entre personas puedan ser rastreadas o conocidas por otras. Los hackers y crackers se valen de esta información para realizar ataques y defraudaciones.

[117] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 142
[118] Cada actividad que se haga en Internet queda registrada en una base de datos, dejando así un rastro de la actividad que cada usuario realiza en la red.

En este punto, si la información no es manejada correctamente por las empresas y sitios que manejan datos puede vulnerarse de manera notable el derecho a la intimidad. Por ello es de suma relevancia que la información, sobre todo la producida entre una entidad bancaria y su usuario, se mantenga de manera confidencial entre las partes, por ejemplo con sistemas de encriptación y protocolos SSL.

c) Integridad:

Para que un intercambio de datos sea considerado seguro, es necesario que el mensaje generado no pueda ser alterado o modificado de ninguna manera. La persona que lo produce debe estar segura de que su mensaje va a ser recibido íntegramente por la otra parte, sin que su voluntad se vea cambiada de forma involuntaria.

La integridad es particularmente importante pues al utilizarse la Internet como un nuevo medio para realizar negocios jurídicos, el mensaje que se genere entre las partes va a ser su contrato, va a producir obligaciones y derechos, y por lo tanto, deben quedar estrictamente protegidos los datos que se hayan elaborado para tal fin.

Como se verá adelante, existen métodos tecnológicos los cuales permiten que un mensaje quede debidamente asegurado y se registre cualquier alteración, volviendo inválido el dato que haya sido modificado una vez que fue enviado por una parte con la garantía de integridad.

d) No repudio:

Esta figura es consecuencia de los puntos a) y c) e implica que las comunicaciones o mensaje que se derive entre las partes no puede ser rechazado o negar su existencia. De este modo, la figura del "no repudio" es considerada como propia de los contratos, como defensa ante la actuación del contratante, que trate de negar la fuerza o validez de un mensaje, acto o contrato[119].

El no repudio implica que lo ofrecido por una de las partes sea obligatorio y no pueda ser desvirtuado. Es decir, que ni el emisor ni el receptor del mensaje puedan negar la transmisión[120]. Con esta figura se busca resguardar la seguridad en las relaciones contractuales, otorgando protección a la parte que pudiera ser perjudicada por el rechazo arbitrario sobre la validez y legitimidad de un determinado mensaje, acto o contrato[121].

[119] RAMOS SUÁREZ, Fernando. Citado por LÓPEZ CHAVARRI, José Francisco. op. cit. P. 144.
[120] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel. op. cit. P. 245.
[121] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 144 y 145.

Esta figura puede presentarse en dos categorías[122]:

1) El no repudio de origen: funciona en beneficio del receptor del mensaje, se presenta en dos supuestos, cuando el emisor niegue el envío del mensaje o cuando el emisor niegue el contenido del mensaje (en todo o en parte).

2) El no repudio de envío: funciona en beneficio del emisor del mensaje, se presenta cuando el receptor pretende negar ya sea una parte o todo el contenido de un determinado mensaje al emisor.

i. Alternativas de seguridad

Para asegurar al consumidor un adecuado manejo de sus transacciones en Internet y brindarle un medio seguro que le genere confianza existen distintas alternativas tecnológicas que hoy funcionan como mecanismos para proteger al usuario y a los sistemas de las empresas.

[122] Ibídem. P. 145.

Estas alternativas buscan asegurar los cuatro elementos anteriormente mencionados que son la meta en el tema de seguridad, en resumen: la autenticidad, la confidencialidad, la integridad y el no repudio.

Los ataques que pueden generarse a la seguridad de los sistemas pueden clasificarse en[123]:

1) **Ataques pasivos:** en este tipo de ataques, el atacante no altera la comunicación, sino que la monitorea o accede a ella con el fin de obtenerla, el objetivo es interceptar la información y el análisis del tráfico. Estos ataques son difíciles de detectar, pues no provocan alteración de los datos, pero sí es posible evitarlos mediante el cifrado de los mensajes, que será explicado adelante.

2) **Ataques activos:** en este tipo de ataques, el atacante sí altera la información. Se puede dividir en cuatro categorías: suplantación de identidad (el intruso se hace pasar por alguien más), reactuación (uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no autorizado), modificación de mensajes (el atacante varía los datos transmitidos) y degradación fraudulenta del servicio (el intruso intenta impedir que los entes dialogantes puedan realizar

[123] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel. op. cit. P.243.

correctamente su función, mediante la destrucción o retardo de mensajes o la introducción de mensajes espurios con el fin de congestionar la red).

Para evitar que se lleven a cabo este tipo de ataques, es importante utilizar una serie de mecanismos que se encuentran disponibles en el mercado y aplicarlos al comercio electrónico, en especial, a la Banca por Internet.

A continuación, se presenta un cuadro que incluye las propuestas de seguridad con la que debe contar un sitio web para considerarse, actualmente, seguro en el comercio electrónico:

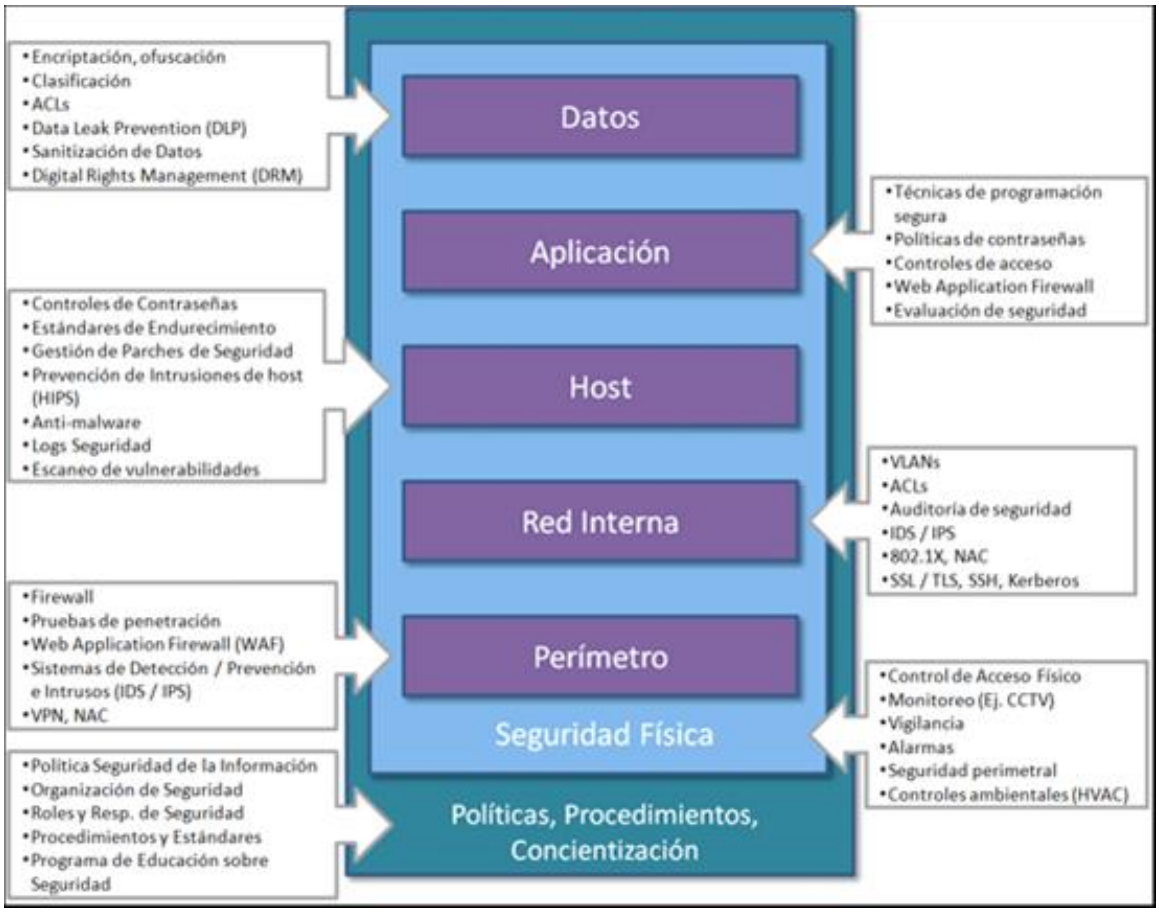


Figura 1. Seguridad en el E-Commerce[124]

[124] AGUILAR Magdalena (2009). "Mesa Redonda: Desafíos de la protección de datos personales en el ámbito bancario y financiero: Derechos del Usuario del comercio electrónico". IX Jornadas de AUSBANC Internacional: Nuevos Derechos Financieros del Siglo XXI. San José, Colegio de Abogados. 01 de octubre de 2009.

A) TECNOLOGÍAS

1. La Criptografía o Encriptación:

Este es uno de los instrumentos que mayormente se utilizan y su objetivo es mantener las comunicaciones en forma privada, de acceso sólo para las partes, protegiendo su contenido de terceras personas. Así, la información es sólo inteligible por las partes directamente involucradas o aquellas que estén autorizadas, ya que se encuentra cifrada. Se afirma que la criptografía es el arte de transformar los contenidos de un mensaje en su forma original, a un mensaje que no puede ser traducido ni decodificado por las partes, sino valiéndose de una clave especial[125].

Entonces, la criptografía viene a ocultar o transformar un mensaje para que solamente puedan leerlo y entenderlo las partes interesadas, para todos los demás, el mensaje contiene una serie de datos sin sentido que no pueden ser comprendidos, pues para "descifrarlos" es necesario tener una clave dada para este fin.

> *"La criptografía cumple funciones muy importantes porque identifica y atribuye el mensaje a una parte precisa, ya que para establecer la*

[125] GLOSARICH, R. citado por RODRÍGUEZ AZUERO, Sergio. op. cit. P. 246.

comunicación se requiere haber intercambiado información. Además, sólo la otra parte puede enviar el mensaje, en la medida en que los terceros a la relación, no tienen conocimiento de la clave".[126]

Con este mecanismo se asegura el cumplimiento del elemento de seguridad Confidencialidad o Privacidad. La encriptación es un mecanismo general de seguridad, para permitir el manejo de datos en Internet, en virtud del cual, el mensaje original se convierte en un lenguaje construido con base en algoritmos basados en fórmulas matemáticas, con lo cual si alguien lo intercepta en el camino, desconoce directamente su contenido, pues es necesario descifrarlo a su recibo en el lugar de destino[127].

Existen distintos tipos de Criptografía, por ejemplo la Criptografía de Llave simétrica o privada y la criptografía de llave asimétrica o pública. Estas modalidades serán brevemente explicadas a continuación.

[126] RODRÍGUEZ AZUERO, Sergio. op. cit. P. 246.
[127] Ibídem.

a) Criptografía de Llave Simétrica o Privada:

Este tipo de encriptación consiste en que, tanto el emisor como el receptor de una comunicación, van a necesitar de una llave o cifrador que ambos deben conocer y utilizar. De este modo, para que un mensaje sea elaborado por una parte y recibida por otra, el emisor debe cifrar el mensaje con la llave y posteriormente el receptor va a utilizar la misma llave para descifrar o desencriptar el mensaje.

Así, se asegura que la información transmitida de una fuente a otra no va a ser vista por nadie más, resguardando así la confidencialidad de las comunicaciones. Esta técnica es considerada segura ante ataques cripto-analíticos sencillos[128].

b) Criptografía de Llave Asimétrica:

En este tipo de encriptación, se utilizan dos tipos de llaves, a diferencia de la criptografía de llave simétrica, una denominada llave privada que va a poseer de manera exclusiva una de las partes, y otra llamada llave pública, que se encontrará disponible para la otra parte y que se adquiere a través de un repositorio. Así, cada persona va a poseer

[128] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 152.

un par de llaves, la llave pública que se encuentra en el repositorio al alcance de todo posible usuario, y la llave privada, que sólo posee la persona.

En este sistema, el único requerimiento es que cada llave pública debe estar asociada a una identidad siguiendo un proceso de reconocimiento fiable[129]. Cada una de las llaves tiene la función de codificar y descodificar el mensaje, por ejemplo, el emisor puede ser quien posea la llave pública, y la utiliza para cifrar un mensaje que envía a un receptor; entonces este receptor debe utilizar la llave privada para descifrar el mensaje enviado, ya que dichas llaves están elaboradas para que únicamente coincidan los algoritmos elaborados para su par. De esta manera, el mensaje sólo puede ser descifrado por quien posea el otro juego de llave correspondiente a un par, y en el caso de un receptor con llave privada, es él quien de modo exclusivo puede tener acceso al contenido del mensaje, pues es quien tiene la herramienta para desencriptarlo.

Dependiendo de quien sea el emisor del mensaje, así será cifrado con una llave pública o con una llave privada, lo mismo sucede para descifrarlo, depende de quien sea el receptor y qué juego de llaves maneje. Como se mencionó en el párrafo anterior, cada juego de llaves está elaborado para que solamente la llave pública correspondiente pueda desencriptar un mensaje encriptado por la llave privada y viceversa.

[129] RODRÍGUEZ AZUERO, Sergio. op. cit. P. 247.

Gracias a esta metodología, la encriptación asimétrica permite que los usuarios puedan enviar un mensaje cifrado sin tener que intercambiar, en momento alguno, una clave común. A pesar de que existe una relación matemática común entre los algoritmos de las llaves (pública y privada), la misma resulta ser muy compleja de modo que resulta en extremo complicado el poder deducir un algoritmo a partir de otro[130], por lo que la seguridad que brinda este mecanismo se encuentra dentro de las mejores calificadas.

Este tipo de encriptación es utilizada para la Firma Digital, como se verá más adelante. Con ella se garantiza la protección de la información, en el caso en que el emisor cifre la información con una llave pública, en cuyo caso el mensaje sólo podrá ser descifrado por el receptor con una llave privada, brindando entonces la seguridad de que dicho mensaje únicamente va a poder ser desencriptado por el receptor.

[130] Ibídem. P. 153.

2. Protocolo SSL (Secured Socket Layer)

La información en Internet se maneja a través de lo que se denomina como protocolos. El protocolo de transferencia de hipertexto[131] HTTP (*Hyper Text Transfer Protocol*) es el que se utiliza en cada transacción de la *Web*. Este tipo de protocolo utiliza, para poder realizar sus aplicaciones, el protocolo TCP/IP, que permite el transporte y el enrutamiento de la información[132].

El SSL *(Secured Socket Layer)* es un protocolo utilizado para permitir que las comunicaciones enviadas por Internet sean manejadas de forma segura. Este se aplica sobre el TCP/IP y debajo del HTTP. Así, realiza una codificación de los mensajes antes de enviarlos por la red. Una vez establecida la comunicación, al momento en que se va a enviar la información, la capa SSL la recoge y la codifica para luego enviarla; posteriormente, el computador destino se encarga de decodificar el mensaje y lo convierte nuevamente en texto original[133].

Este protocolo proporciona autenticación y confidencialidad en las comunicaciones por Internet, y una vez que es aplicado se muestra bajo la denominación

[131] Hipertexto, en informática, es el nombre que recibe el texto que en la pantalla de una computadora conduce a otro texto relacionado. Wikipedia (2009). http://es.wikipedia.org/wiki/Hipertexto. [Consulta del 27 de noviembre de 2009].
[132] LÓPEZ CHAVARRI, José Francisco. op. cit. PP. 156 y 157.
[133] Ibídem.

HTTPS, que implica que el protocolo HTTP está siendo utilizado junto con el protocolo SSL. La mayoría de los bancos que prestan el servicio de banca por Internet utilizan el protocolo SSL, e incluso recomiendan que una de los cuidados que debe tener todo usuario de banca *online* es asegurarse que la dirección del banco aparezca precedida del formato HTTPS, por ejemplo[134]:

https://www.bnonline.fi.cr/Login/

https://www.personas.bancobcr.com/plantilla/

https://www.popularenlinea.fi.cr/bpop

Los TLS (*Transport Layer Security*) son, al igual que los SSL, protocolos de seguridad para el transporte de las comunicaciones, pero un poco más avanzado, aunque con la misma función de realizar un cifrado de la información y asegurar las comunicaciones por la red Internet.

SSL implica una serie de fases básicas[135]:

1) Fase de Saludo o *Handshacking*: consiste en la identificación de los dos interlocutores, que se presentará cuando las computadoras verifican la

[134] La primera dirección corresponde a la página de inicio de sesión en Internet Banking personal del Banco Nacional, la segunda corresponde, en el mismo sentido, a la del Banco de Costa Rica y la tercera a la del Banco Popular. [Consulta del 03 de diciembre de 2009].
[135] LÓPEZ CHAVARRI, José Francisco. op. cit. PP. 157 y 158.

identidad de sus usuarios, comprobando que ambos cuentan con certificados válidos. Se da el intercambio de claves públicas y se confirman las identidades de las partes, entonces, en este momento, los sistemas escogen una clave de sesión tipo simétrico para transmitir la información en la comunicación.

2) Fase de comunicación: en esta fase se produce el intercambio de la información utilizando la llave de sesión acordada en la fase anterior.

3. Sistemas de Detección/Prevención de Intrusos (IDS/IPS)

El IDS *(Intrusion Detection System)* es un programa que se utiliza para detectar accesos no autorizados a una computadora o a una red[136]. Este mecanismo fue utilizado en inicios de la Banca por Internet por el Banco de Costa Rica:

> *"Cuando se contrató el servicio de Banca por Internet se contrató bajo el sistema de llave en mano entonces el proveedor fue el que se encargó de dar la opción debidamente asegurada, un equipo de firewall de por medio, lo que en aquel entonces se consideraba necesario, no existían los famosos IPS como*

[136] Wikipedia (2009). http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos.[Consulta del 29 de noviembre de 2009].

preventores de intrusos sino que existían los IDS entonces se colocaron IDS y el sistema de autenticación era básicamente usuario y clave, que era lo que se consideraba seguro en ese entonces."[137]

Según explica el Ingeniero en Sistemas Max Alvarado[138], los IDS son elementos que se ponen de forma pasiva en una red, y lo que hacen es que el tráfico que está yendo del punto A al punto B se replique, para que también llegue a este módulo; entonces lo que los IPS hacen es ir monitoreando la información que va pasando para darse cuenta si se está dando un ataque, lo que pasa con ellos es que cuando se da cuenta que se está dando un ataque, éste efectivamente ya se estaba dando, ya era efectivo, entonces en realidad era post mortem. Se utilizaba para saber cuándo fue que se dio el ataque, cómo fue que se dio y tal vez tratar de rastrear al causante del hecho.

Es por ello, que debió avanzarse dentro del esquema de seguridad para incorporar un instrumento que ayudara a prevenir los ataques, en lugar de únicamente detectarlos cuando ya habían sido consumados. Así, se implementó el uso de los denominados IPS.

El IPS (*Intrusion Prevention System*) es un dispositivo que funciona como prevención de intrusos en el sistema, de modo tal que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La

[137] SEBIANI SERRANO, Alejandro (2009). Gerente de Seguridad en Tecnología del Banco de Costa Rica. Entrevista Sucursal Banco de Costa Rica, Barrio Tournon. 14 de setiembre de 2009.
[138] ALVARADO, Max (2009). Ingeniero en Sistemas. Entrevista en CISCO Systems, Plaza Roble. 06 de octubre de 2009.

tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos (firewall)[139].

El Ingeniero Max Alvarado, explica de esta manera el funcionamiento del IPS:

> *"El IPS se coloca de una forma en la que el tráfico de A a B tiene que pasar a través de él antes de llegar a B, entonces lleva un escaneo más en línea. Antes que llegue al servidor de destino la información es filtrada y cuando se detecta un ataque se bloquea en el momento, esto es como seguir el patrón de los datos que están llegando para determinar si es un ataque o no, por ende requiere un proceso de actualización, hay que estar como con el antivirus pendiente de nuevos ataques, de estar actualizando las firmas para que se puedan hacer los bloqueos. Efectivamente los IPS son bastante efectivos y eficientes para detener ataques."*[140]

Este mecanismo es ahora utilizado por algunos bancos, pues resulta actualmente, según se manifestó en diversas entrevistas y tal como se muestra en la figura 1, como uno de los instrumentos necesarios para una banca en línea catalogada como segura. Es para

[139] Wikipedia (2009). http://es.wikipedia.org/wiki/Sistema_de_Prevenci%C3%B3n_de_Intrusos. [Consulta del 29 de noviembre de 2009].
[140] ALVARADO, Max (2009). Ingeniero en Sistemas. Entrevista en CISCO Systems, Plaza Roble. 06 de octubre de 2009.

muchos, uno de los requisitos indispensables para desarrollar un servicio por Internet de manera segura.

4. Firewall (Cortafuegos/ Muros de Fuego)

El Firewall (o cortafuegos) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios[141].

Los firewall son dispositivos de control de acceso para la red y pueden ayudar a proteger la red interna de una organización contra ataques externos. Por su naturaleza, los firewall son productos de seguridad de frontera, lo cual significa que están en el límite entre la red interna y la red externa. Si son configurados de manera apropiada, los "muros de fuego" se convierten en dispositivos de seguridad indispensables. Sin embargo, un corta fuegos no evitará que un atacante utilice una conexión permitida para atacar un sistema. Por ejemplo, si un servidor web tiene permitido el acceso desde el exterior y es

[141] Wikipedia (2009). http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica). [Consulta del 29 de noviembre de 2009].

vulnerable a un ataque en contra del software del servidor web, es probable que el firewall permita pasar el ataque, pues se supone que el servidor web debería poder recibir conexiones web. Los firewall tampoco protegerán a una organización de un usuario interno, puesto que dicho usuario ya se encuentra en la red interna[142].

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados[143].

Existen dos tipos generales de muros de fuego, los muros de fuego de capa de aplicación y los muros de fuego de filtrado de paquetes[144].

[142] MAIWALD, Eric. op. cit. P. 12
[143] Wikipedia (2009). http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica). [Consulta del 29 de noviembre de 2009].
[144] MAIWALD, Eric. op. cit. P. 214.

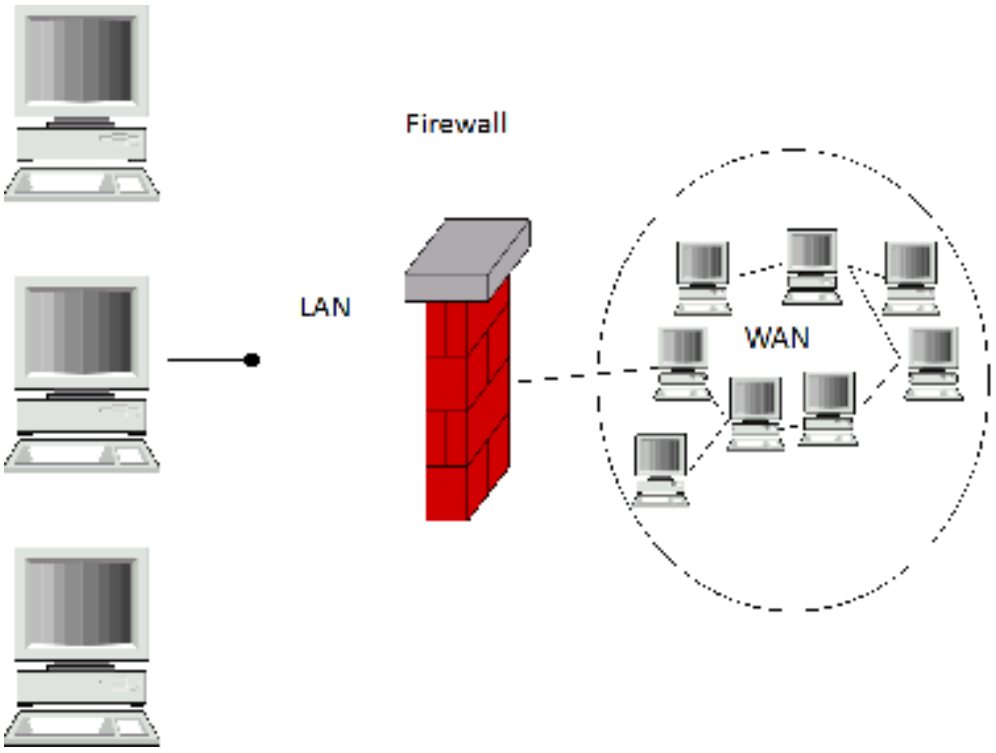


Figura 2. Firewall (Cortafuegos) [145]

[145] Wikipedia (2009). http://es.wikipedia.org/wiki/Archivo:Gateway_firewall.svg. [Consulta 29 de noviembre de 2009].

W.A.N. (Red de área extensa): Red que abarca un área geográfica más amplia que una red de área local (L.A.N.) sobre redes de comunicaciones públicas.
L.A.N. (Red de área local): El término "red de área local" (LAN) hace referencia a una red local o un grupo de redes locales interconectadas que están bajo el mismo control administrativo. En los comienzos del networking, las LAN se definían como redes pequeñas que existían en una única ubicación física. A pesar de que las LAN pueden ser una única red local instalada en una vivienda u oficina pequeña, la definición de LAN ha evolucionado y ahora incluye redes locales interconectadas compuestas por muchos cientos de hosts, instaladas en múltiples edificios y ubicaciones.
Ambos conceptos tomados de:
Cisco Networking Academy (2009). <http://www.cisco.com/web/learning/netacad/index.html>. [Consulta del 4 diciembre 2009].

5. Firma digital y certificado digital

a. Firma Digital

Es necesario, antes de abordar el tema de firma digital, diferenciar entre firma electrónica y firma digital. Para ello, simplemente debe anotarse que la firma electrónica es el género y la firma digital es la especie[146]. La firma electrónica es definida como cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita[147]. En términos sencillos, la firma electrónica es la que se introduce en un documento electrónico[148] con el fin de acreditarse su autoría y que de este modo se pueda identificar al titular de la firma con relación con el mensaje que se está enviando. Con la firma electrónica se permite hacer una relación o asociación entre un documento electrónico y una persona.

[146] MORENO NAVARRETE, Miguel Angel. Citado por MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA. op. cit. P. 251.
[147] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 164.

[148] Documento Electrónico: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático. Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Nº 33018 de 27 de marzo del 2006, reformado, artículo 2 inciso 21.

Dentro del concepto de firma electrónica se comprenden otras formas de identificación, entre ellas, como se mencionó *supra*, la firma digital. El concepto de firma digital se asocia con el desarrollo de tecnologías PKI o ICP (*Public Key Infrastructure* o Infraestructura de Clave o Llave Pública, según su denominación en inglés o español), incluso, la utilización de este tipo de tecnologías es lo que hace que la firma digital sea distinta a la firma electrónica, en el tanto la primera utiliza la criptografía de clave pública y la segunda cualquier tipo de criptografía.

Las firmas digitales han sido clasificadas de la siguiente manera[149]:

b. *"Blind Signature"* (Firma Ciega): es un protocolo de firmas digitales que permite firmar un documento sin conocimiento de los contenidos del mensaje.
c. *"Fail-stop Signature"* (Firma que detecta errores): le permite al tenedor demostrar que una firma en un documento le es falsamente atribuida, ya que es producto de un ataque.
d. *"Proxy Signature"* (Firma Proxy): es un protocolo que le permite al firmante autorizar a otro para que firme en su nombre, sin tener que revelar para esto su llave privada.

[149] SCHNEIER, citado por LÓPEZ CHAVARRI, José Francisco. op. cit. P. 169.

e. *"Undeniable Digital Signature"* (Firma Digital Innegable): es un protocolo que no permite la verificación de la firma sin el consentimiento del signatario.

Para la utilización de la Firma Digital se requiere de dos tipos de llaves: una llave pública, accesible a cualquier persona y una llave privada, que va a ser utilizada de forma exclusiva por el dueño, tal y como se explicó con la Criptografía de Llave Asimétrica.

El fin principal de la firma digital es brindar seguridad a las transacciones electrónicas, protegiendo de esta manera la información, a través del cifrado que se genera con la utilización de llaves públicas y llaves privadas para la transmisión de la comunicación. También, se garantiza la identidad de los sujetos, ya que se conoce quién es la persona que se atribuye un mensaje y se puede identificar claramente.

El mensaje que el emisor pretende enviar con firma digital, es sometido a una serie de operaciones matemáticas denominadas funciones *hash*[150], que se utiliza tanto para crear como para verificar la firma digital. Esta función garantiza el contenido original del mensaje, y ofrece la garantía efectiva de que el mensaje no ha sido modificado desde que

[150] Esta función es un proceso matemático basado en un algoritmo que crea una representación numérica o forma comprimida del mensaje original (*message digest*), en forma de un valor control de una longitud estándar que suele ser menor que la del mensaje, pero que es esencialmente única con respecto al mismo. Todo cambio en el mensaje produce invariablemente un valor control distinto cuando se utiliza la misma función *hash*. LÓPEZ CHAVARRI, José Francisco. op. cit. P. 154.

se firmó digitalmente, lo que adiciona uno de los elementos de seguridad que se busca al realizar las transmisiones de datos: la integridad del mensaje[151].

Una vez que se aplica la función *hash* al mensaje original, se genera el *message digest*, que será el indicador para comprobar cualquier alteración del mensaje, pues realiza un análisis completo del contenido verificando si concuerda con el mensaje original de acuerdo con el valor único *hash*, de modo tal que cualquier alteración, por más mínima, va a producir un valor *hash* totalmente distinto al que tuvo el mensaje original[152].

Cuando se tiene el *message digest*, este es sometido a la encriptación por medio de la llave privada del sujeto que emite el mensaje, y ahí es donde se produce la Firma Digital. Una vez enviada la comunicación con la firma digital incluida, el receptor deberá realizar dos operaciones, en primer lugar, debe verificar la identidad del emisor, y en segundo lugar, debe determinar si el mensaje fue alterado. Para hacer lo primero, el receptor deberá acceder a la llave pública del emisor, en un repositorio[153] de llaves públicas, y procederá a desencriptar la firma digital del emisor recordando que únicamente la llave pública puede desencriptar un mensaje encriptado con la llave privada. Si logra desencriptar la firma que se encuentra en el documento, se comprobará

[151] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 154.
[152] Ibídem.
[153] Repositorio: Sistema de almacenamiento y distribución de certificados e información relacionada. Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Nº 33018 de 27 de marzo del 2006, reformado, artículo 2 inciso 41.

la identidad del emisor (identificación). Para lo segundo, el receptor deberá aplicar la misma función *hash* al mensaje que se le envió, y si el resultado es exacto al *message digest* anejo al documento, entonces se comprobará que el documento no ha sido alterado, garantizando el no repudio[154].

En resumen, la firma digital garantiza los elementos de seguridad de autenticidad, integridad, confidencialidad y no repudio. Cada vez que se requiera firmar digitalmente un documento se producirá una firma distinta, ya que cada firma digital es única e irrepetible. Esto no le resta validez, pues el receptor del mensaje puede constatar que la firma aplicada al documento corresponde a la persona que lo emitió, utilizando la llave pública correspondiente, y si ambas llaves coinciden (la privada con la que se firmó y la pública para descodificar el mensaje) no existe ningún problema en que una persona pueda tener varias firmas digitales, pues todas pueden ser objeto de reconocimiento formal.

Se pretende que un documento que posea una firma digital tenga la misma validez que un documento con firma manuscrita, cuestión que ha sido expresamente manifestada en la Ley Modelo de la CNUDMI (UNCITRAL) y que ha sido abordado en los distintos proyectos de firma digital creados a nivel mundial, siendo que Costa Rica no ha

[154] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 155.

sido la excepción, pues en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454 en el artículo 9 se estipuló lo siguiente:

> *"Artículo 9º—Valor equivalente. Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.*
>
> *Los documentos públicos electrónicos deberán llevar la firma digital certificada."*

Para la aplicación de la firma digital se recurre a una tercera parte, que va a intervenir en el proceso de comunicación asegurando la autenticación y confidencialidad del mismo; este papel lo desempeñan las Entidades Certificadoras o Autoridades de Certificación. Las Entidades Certificadoras generan la confianza para el establecimiento de relaciones comerciales entre partes desconocidas, con la implementación de normas y directrices técnicas en las transacciones[155].

Las entidades certificadoras funcionan bajo el sistema de "Infraestructura de Clave Pública", que se relaciona con todo un nivel jerárquico de entidades certificadoras en

[155] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 171.

donde las de niveles superiores certifican a las de niveles inferiores y con esto se reconoce el proceso de validación que éstas realizan. Para fungir como entidad certificadora existen una serie de requisitos con los que se deben cumplir, y que están establecidos en detalle en la Ley de Certificados, Firmas digitales y su Reglamento

b. Certificado Digital

La certificación es una respuesta al problema de autenticidad, ya que existen entidades dedicadas a esa labor y que brindan esa credibilidad necesaria para el consumidor de servicios electrónicos.

Los certificados y claves de acceso son producto de la combinación de un mecanismo de creación que se encuentra en poder del firmante y de un mecanismo de verificación que se encuentra en poder de un tercero de confianza que certifica identidad y contenido, al que la ley denomina "certificador", conocidos también como *Public Key Certificates* (Certificados de llave pública).

A pesar de que, con la firma digital, se asegura que una clave pública del suscriptor corresponda a su clave privada, se hace necesario que exista un ente que dé mayor

legitimación a este par de números y con certeza afirme la asociación de un par de llaves a una persona determinada.

En el tema de seguridad, como se ha comentado, las técnicas deben garantizar el máximo de protección posible, previniendo fallas que puedan provocar ataques. Así, a pesar que la firma digital proporciona muchas ventajas, si no existe un medio adecuado para su utilización podría vulnerarse su nivel de seguridad. Es por ello, que debe complementarse su uso con un tercer agente participante, que va a administrar las claves y a emitir certificados individualizando y relacionando una clave pública con una persona determinada. La presencia de un tercero es lo que permite sostener la plena seguridad e inviolabilidad de las expresiones volcadas en este tipo de soporte[156].

Los certificados digitales son emitidos por una autoridad competente que posee un registro en el que guarda la identidad de la persona que lo posee, su vigencia, lugar de emisión, entre otros. Las entidades certificadoras administran las claves, emiten certificados individualizando y relacionando una clave pública con un tenedor específico. Estos certificados son inscritos por la entidad certificadora en un registro o receptorio,

[156] MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel. op. cit. P255.

deben acompañar a los documentos o mensajes, de forma tal que el que los recibe pueda, con la clave pública del firmante, corroborar la vigencia del mismo[157].

Las funciones de los certificados digitales pueden enumerarse de la siguiente manera[158]:

i) otorgar certeza de determinadas circunstancias fácticas: por ejemplo, certificando la identidad del signatario y dueño de la clave privada.

ii) determinar la eficacia de ciertos actos ejecutados por una persona en particular: por ejemplo, la certificación de un contrato de mandato para la realización de un acto determinado.

Pero la función básica del Certificado Digital es vincular una clave pública con un tenedor determinado, lo que le permite al receptor asegurarse que la clave pública consta en el certificado y corresponde a la clave privada utilizada para firmar el documento. Para asegurar la autenticidad del certificado, la entidad certificadora firma el certificado con su propia firma. Esta última se puede verificar utilizando la clave pública de la entidad siguiendo el esquema de ICP (Infraestructura de Clave Pública), que se encontrará

[157] Ibídem.
[158] LÓPEZ CHAVARRI, José Francisco. op. cit. P. 175.

certificada por una entidad certificadora de mayor jerarquía (aunque podría ser de la misma jerarquía) y así sucesivamente[159].

El contenido que puede tener un certificado digital dependerá del tipo y función del certificado, y de los requisitos legales que le sean exigidos. En el certificado digital suelen incluirse dos posibilidades, la firma digital y la autenticación.

Las entidades certificadoras incluyen cada certificado que se emita con su correspondiente llave pública en un Repositorio, que consiste en un registro accesible al público en el que se puede con facilidad verificar que cada llave pública corresponde a una persona determinada. Los repositorios son bases de datos electrónicas en línea, que permite la verificación de los certificados, su validez, y otro tipo de información que pueda utilizarse para verificar la identidad del dueño del par de llaves.

Cada certificado posee una vigencia determinada, y una vez vencido este plazo, si no existe inconveniente, puede renovarse el certificado. El certificado es emitido por la entidad certificadora cuando se comprobó íntegramente la identidad del solicitante, aunque no siempre la emisión y la identificación recaen en la misma entidad.

[159] Ibídem. P. 176

Los beneficios que proporcionan los certificados digitales son principalmente[160]:

- Sirven para identificarse ante terceros, previniendo la suplantación de la identidad en Internet.
- Garantizan la identidad del emisor y del receptor de la información, así como la inalterabilidad del mensaje que se transmite.
- Proporciona confidencialidad, en la medida que sólo el emisor y el receptor pueden leer la información guardada en el documento (se encripta la comunicación).

Los certificados pueden tener diferentes grados de "calidad", dependiendo de la labor de identificación del suscriptor del certificado. Cada entidad debe publicar los procedimientos que se siguen para la identificación y emisión de los certificados, con el fin de demostrar esa calidad[161].

Cada participante dentro del esquema de expedición del certificado digital tiene una responsabilidad diferente, así[162]:

[160] RODRÍGUEZ AZUERO, Sergio. op. cit. P. 248.
[161] Ibídem.
[162] Ibídem.

- La entidad de certificación responde por emitir de forma segura e irrepetible el par de llaves –pública y privada-, así como de guardar su propia clave privada y garantizar la calidad técnica del equipo informático.
- La autoridad de registro (repositorio) es responsable de identificar completamente al usuario, siéndolo directamente de los datos que certifica.
- El titular del certificado debe notificar las modificaciones en los datos certificados, la pérdida de la tarjeta inteligente donde se guarda el certificado o cualquier incidencia que conozca.

Existen varios tipos de certificados digitales, por ejemplo[163]:

- Certificado de Representación de Empresa/Entidad: se expide a personas naturales nacionales o extranjeras que se han identificado plenamente con la calidad de representante legal de una persona jurídica o Entidad del Estado.

- Certificado de Pertenencia a Empresa/Entidad: se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante como perteneciente a una determinada organización empresarial o entidad del Estado,

[163] CERTICÁMARA S.A. (2009). http://web.certicamara.com/certificados-digitales-firma.aspx. [Consulta del 07 de diciembre de 2009].

pero sin que tenga la representación legal de la misma o facultad de comprometerla jurídicamente.

- Certificado de Titular de Función Pública: se expide a personas naturales nacionales o extranjeras que se han Identificado plenamente como funcionario público perteneciente a una entidad del Estado.

- Certificado de Profesional Titulado: se expide a personas naturales nacionales o extranjeras que se han identificado plenamente y que hayan obtenido el correspondiente registro, licencia, colegiatura o tarjeta profesional requerida para el ejercicio de su profesión en un país determinado o en un Estado Extranjero.

- Certificado digital persona natural: se expide a personas naturales nacionales o extranjeras que se han identificado plenamente con documento(s) equivalente(s) expedido(s) por la registraduría y cuentan con Cedula de Ciudadanía.

- Certificado para Firma de Código: permite a una persona jurídica o natural firmar mensajes de datos que contengan información, software, aplicativos, código fuente o código objeto para garantizar ante terceros que el software es distribuido están aprobados por su propietario y no han sido alterados.

- Certificado de Persona Jurídica Entidad/Empresa: es un tipo de Certificado Digital que identifica a una persona jurídica de derecho público o privado, o entidad del Estado. Garantizando: (i) que una persona jurídica determinada se ha identificado como tal y ha solicitado el servicio a través de su representante legal, y (ii) que esa persona jurídica podrá programar un sistema de información para que firme digitalmente mensajes de datos, de manera automática o manual, vinculándose jurídicamente.

Los certificados digitales pueden ser suspendidos, revocados, renovados, entre otras situaciones, todo según lo disponga la legislación correspondiente al respecto, con una serie de procedimientos para cada trámite.

B. RIESGOS

El riesgo puede definirse como aquello que puede ser permitido y requiere protección[164]. A nivel de seguridad es un elemento que no puede dejarse jamás de lado y debe evaluarse constantemente. La seguridad va de la mano con el riesgo, pues si no existiera riesgo no sería necesaria la seguridad.

Dentro del riesgo deben analizarse dos conceptos: la vulnerabilidad y la amenaza[165].

a. Vulnerabilidad: una vulnerabilidad es una vía de ataque potencial. Ella se caracteriza por la dificultad y el nivel de capacidad técnica que se requiere para explotarla.

b. Amenaza: una amenaza es una acción o evento que puede violar la seguridad de un entorno de sistemas de información. Existen tres componentes de la amenaza:

1. Objetivos: el aspecto de la seguridad que puede ser atacado

[164] MAIWALD, Eric. op. cit. P. 144.
[165] Ibídem, PP. 144 y 145.

2. Agentes: Las personas u organizaciones que originan la amenaza

3. Eventos: El tipo de acción que representa la amenaza.

Toda organización debe analizar constantemente sus sistemas y estar vigilante ante cualquier riesgo, tomando en cuenta sus elementos y adoptando medidas de seguridad que minimicen esos canales de peligro. Debe tenerse presente que el Internet es inseguro, el riesgo nunca va a eliminarse por completo, pero sí puede prevenirse y trabajar en técnicas que lo minimicen.

Sergio Rodríguez Azuero[166] afirma que si el banco tiene unos riesgos asociados a la prestación directa de servicios bancarios a sus clientes, ellos se incrementan de manera sensible cuando se producen en apoyo del comercio electrónico.

Aquí se vuelve vital la constante evaluación del riesgo y la renovación constante en los sistemas de seguridad, procurando mantenerse a la vanguardia en la utilización de sistemas tecnológicos, búsqueda de capacitaciones, información a los usuarios, entre otros, como elementos primordiales para la estructura de seguridad de la entidad.

[166] RODRÍGUEZ AZUERO, Sergio. op. cit. P. 242.

C. CONCIENTIZACIÓN

Este aspecto es vital en la seguridad y, sin embargo, ha sido el menos explotado. En el tema de Políticas y procedimientos, la concientización toma un papel determinante, pues se requiere que el usuario se encuentre debidamente informado de sus deberes y obligaciones en el comercio electrónico, máxime cuando la tecnología utilizada para brindar seguridad requiere de un conocimiento cada vez más amplio y la adecuada comprensión del papel que cada actor desempeña, con adecuado manejo de sus responsabilidades.

Los expertos insisten en que no es suficiente una tecnología en seguridad con los máximos niveles si el consumidor no tiene educación sobre su papel y los cuidados que debe tener en Internet. De nada vale contar con los mecanismos más avanzados si el cliente no se encuentra debidamente capacitado para hacer el uso correcto de ellos y de este modo darle la seguridad necesaria a sus operaciones.

3.2 MEDIDAS DE SEGURIDAD: LO QUE ES

i. Legislación

En la legislación costarricense no existe una ley específica que regule el comercio electrónico o la actividad en Internet. Actualmente se encuentra en la Asamblea Legislativa un Proyecto de Ley de Comercio Electrónico, con el número de expediente 16081. La finalidad de este proyecto es regular la actividad comercial producida en medios electrónicos con el fin de brindar mayor seguridad a las transacciones electrónicas. Del mismo se extrae lo siguiente:

> *"Las instituciones y sistemas reguladores del Estado deben garantizar la confianza, protección y seguridad jurídica de las partes involucradas en las transacciones económicas electrónicas. Ante ello la autenticación y seguridad de documentos y mensajes digitales son fundamentales para garantizar a los agentes económicos que sus transacciones tendrán reconocimiento legal y que en caso de que se tengan que dirimir conflictos, se puedan asignar responsabilidades y reparar daños según fuese el caso. En este contexto la introducción de la firma digital en nuestro ordenamiento jurídico por medio*

de la Ley N.º 8554 ha sido el primer paso importante en la dirección apuntada."[167]

Sin embargo, el dictamen 9337 de la Comisión especial de Ciencia, Tecnología e Innovación, con fecha del 19 de noviembre del 2009, se dio una votación unánime negativa con respecto a este Proyecto, por lo tanto fue rechazado.

Adicionalmente, se encuentra también en el Parlamento, el Proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales, con expediente número 16679. Con este proyecto se busca proteger el derecho a la intimidad de las personas mediante el control de los datos personales en la red de Internet, pues éstos pueden ser fácilmente obtenidos y manipulados de manera nociva. Se extrae del proyecto lo siguiente:

"La protección de datos de las personas en la actualidad se constituye en uno de los grandes temas jurídicos que deben ser abordados en la sociedad del siglo XXI. Las tecnologías de la información se constituyen en medios de manejo y difusión rápida de los datos, sin mayor consideración ni control. La realidad costarricense no es ajena a toda una diversa gama de situaciones

[167] Proyecto de Ley de Comercio Electrónico. Expediente Legislativo 16081.

que se presentan con la información que viaja a través de la red de Internet o que la encontramos ubicada en bases de datos públicas y privadas. Frente a esto, debemos tomar en consideración todo lo relativo a la protección de derechos fundamentales de las personas, entre ellos, los derechos de la personalidad y el derecho a la intimidad entre otros."[168]

A este proyecto se le dio Dictamen afirmativo de minoría por la Comisión permanente ordinaria de asuntos jurídicos, según dictamen 8863 del 16 de enero del 2009, calificándolo de "singular importancia" para garantizar el tratamiento adecuado de los datos personales, ya que en ausencia de normativa sobre el particular, la Sala Constitucional se ha encargado de marcar una serie de parámetros al respecto.

Dentro del marco jurídico que rige la materia del comercio electrónico, y en específico de la Banca por Internet, sugiere especial interés la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Ley número 8454 del 20 de agosto del 2005. Esta ley, junto con su reglamento con número 33018, regulan la creación, emisión, tramitación, y manejo en general de los certificados y firmas digitales, así como de los documentos electrónicos. También, se indica el procedimiento y requisitos necesarios para los Certificadores y toda la regulación jerárquica existente al respecto.

[168] Proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales. Expediente Legislativo 16679.

Dicha ley promueve la utilización de mecanismos de seguridad de alto grado tecnológico en la actualidad, cuales son el Certificado Digital y la Firma Digital. Se delega la administración y supervisión del Sistema de Certificación a la Dirección de Certificadores de Firma Digital, que pertenece al Ministerio de Ciencia y Tecnología (MICYT).

Con esta ley, se faculta a las entidades públicas y al Estado a utilizar los certificados, firmas digitales y documentos electrónicos, y dota de plena validez a los certificados expedidos por certificadores registrados en la Dirección de Certificadores de Firma Digital.

En el artículo 19 del Reglamento a la Ley, se indican las atribuciones y responsabilidades de los certificadores, dentro de las cuales destacan:

- Expedir las claves, contraseñas o dispositivos de identificación a sus suscriptores, en condiciones seguras y previa verificación fehaciente de su identidad. Lo mismo hará respecto de sus certificadores subordinados cuando los hubiere, los cuales también deberán registrarse ante la Dirección de Certificadores de Firma Digital.

- El certificador no podrá copiar o conservar información relativa a la clave privada de firma digital de un suscriptor y deberá abstenerse de tomar conocimiento o acceder a ella bajo ninguna circunstancia.

- Llevar un registro completo y actualizado de todos sus suscriptores, para lo cual les requerirá la información necesaria.

- Expedir el certificado digital que respalde la firma digital de los suscriptores de sus servicios y de sus certificadores subordinados, así como suspenderlo o revocarlo bajo las condiciones previstas en la Ley y el Reglamento.

- Mantener un repositorio electrónico, permanentemente accesible en línea y publicado en Internet para posibilitar la consulta de la información pública relativa a los certificados digitales que haya expedido y de su estado actual.

El funcionamiento del certificado y la firma digital se explicó con anterioridad, y se apega al procedimiento que se utiliza en la ley y el reglamento costarricenses. El certificado digital se encontrará en un dispositivo denominado *Smart Card* o Tarjeta inteligente, que consiste en un plástico con un chip denominado placa de contactos y, un circuito integrado que en algunos casos es un microprocesador, lo que le da el carácter de "inteligente"[169]. En las tarjetas inteligentes de microprocesador, que son las utilizadas para certificados y firmas digitales, se puede almacenar información sobre el dueño de la tarjeta, su clave o llave privada, información sobre el certificado como la vigencia, fecha de expedición, entre otros datos.

Figura 3. Tarjeta inteligente o Smart Card[170]

[169] RODRÍGUEZ AZUERO, Sergio. op. cit. P. 232.
[170]SMART CARD (2009). www.smart-card.com/.../smart-card-security.jpg. [Consulta del 08 de diciembre de 2009]

Dentro de la Tarjeta inteligente se coloca el Certificado Digital, que va a permitir realizar dos funciones: firmar digitalmente o la autenticación. La tarjeta detectará la aplicación que se quiera ejecutar dependiendo del sitio o acción que se esté realizando, por ejemplo, si se ingresa a una página bancaria, la Smart Card desplegará la función de autenticación, mientras que si se ingresa a un procesador de texto, la tarjeta iniciará la función de firma digital.

Para utilizar la Tarjeta Inteligente se requiere un lector de Tarjetas Inteligentes o *Smart Card reader* que consiste en un hardware o dispositivo físico que se coloca en la computadora y que requiere además de la instalación de un programa para lectores de tarjetas inteligentes. El dispositivo puede ser insertado a través de un puerto USB, por ejemplo. Los lectores de tarjetas inteligentes están diseñados para descargar o leer los datos de la tarjeta.

Cuando una tarjeta inteligente y un lector de tarjetas inteligentes entran en contacto, cada uno se identifica a sí mismo enviándose y recibiendo información. Si el mensaje intercambiado no concuerda, el proceso no va más allá. Entonces, a diferencia de las tarjetas

bancarias ordinarias, las tarjetas inteligentes pueden defenderse a sí mismas contra usuarios no autorizados y utiliza unos mecanismos de seguridad innovadores[171].

Figura 4. Lector de Tarjetas Inteligentes[172]

Una vez que el usuario ingresa su tarjeta inteligente en el lector, éste le va a solicitar una contraseña, que será la que identifique en un primer plano al usuario como dueño de la tarjeta, este paso es requerido para que el lector proceda a leer la información de la tarjeta inteligente. Debe aclararse que esta contraseña no corresponde a la clave privada, pues ésta ni siquiera es de conocimiento del usuario; la clave privada se

[171] Traducción moderada de SMART CARD (2009). www.smart-card.com/.../smart-card-security.jpg. [Consulta del 08 de diciembre de 2009].
[172] SMART CARD (2009). www.smart-card.com/.../smart-card-security.jpg. [Consulta del 08 de diciembre de 2009].

encuentra guardada dentro del chip de la tarjeta inteligente y no es conocida por nadie. De esta manera se garantiza la confidencialidad y la seguridad de la administración de la clave.

Este tipo de tecnología es lo que los bancos pretenden poner en funcionamiento a muy corto plazo, adicionando estos mecanismos a la seguridad que ofrecen al usuario. Algunos bancos van a incluir este sistema y lo van a hacer de uso obligatorio, otros, sin embargo, lo van a dejar como una opción para el consumidor. La diferencia radica básicamente en una cuestión de costos, pues en el caso particular del Banco Nacional, se ha manifestado que su ideología de banca por Internet siempre ha sido de compromiso social y con el fin de disminuir la brecha digital, de modo que, el obligar a sus clientes a utilizar la firma digital implicaría el disminuirles las posibilidades de acceso a *Internet Banking* a un alto porcentaje de la población, que no cuenta con los medios para cubrir los costos de un lector de tarjetas inteligentes, y demás requisitos que son necesarios para la utilización de este sistema[173].

No obstante, la tecnología de firma digital pretende extenderse y la mayoría de bancos lo ven como el siguiente paso. Incluso se perfila que el certificado digital se encuentre dentro de la cédula de identidad.

[173] CUADRA CHAVARRÍA, Cilliam. Ingeniero informático Banco Nacional. Tomado de entrevista realizada el 16 de setiembre del 2009

Otra ley de relevante importancia para el tema de Banca por Internet es la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (Ley del Consumidor, en adelante) número 7472. De ella se hablará con detalle más adelante, pero no debe dejarse de lado que establece un marco de protección para el consumidor, incluido dentro de esta definición todo usuario de un servicio electrónico, sin excluir la Banca por Internet.

Debe también indicarse, que los bancos han trabajado sus mecanismos de seguridad basados en una serie de Buenas Prácticas, pues no existe un instrumento vinculante que los regule. De este modo, cada quien establece sus medidas de seguridad basándose en distintos esquemas, según el tipo de Banca por Internet que pretendan desarrollar. Dentro de las disposiciones que han tomado en cuenta para elaborar su esquema de seguridad se encuentra el Código de Autorregulación de Buenas Prácticas Bancarias para la Protección de las transacciones efectuadas mediante el uso de instrumentos electrónicos de pago de la Cámara de Bancos e Instituciones Financieras de Costa Rica, que fue elaborado en colaboración de distintas entidades bancarias con el fin de crear una especie de marco referencial para sus esquemas.

Asimismo, son tomadas en cuenta las Normas Técnicas para la gestión y control de las Tecnologías de Información, de la Contraloría General de la República y disposiciones que a nivel internacional se establecen pero a modo de recomendaciones, sin carácter obligatorio.

En la SUGEF existe el reglamento sobre la Gestión de la Tecnología de Información (Acuerdo SUGEF 14-09) que tiene por objeto la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI).

Las disposiciones establecidas en dicho reglamento son aplicables a las entidades supervisadas por la Superintendencia General de Entidades Financieras y al Sistema Nacional de Pagos Electrónicos (*SINPE*).

Este reglamento, sin embargo, no establece de manera específica un lineamiento que incluya las medidas de seguridad que deben adoptar las entidades bancarias para brindar el servicio de Banca por Internet.

A continuación se muestra la tabla de evaluación que se utiliza para las entidades bancarias.

TABLA 14 Banca electrónica

Servicio	**1 S/N**	**Red administrada por**		**conexión en línea directa (on-line)$_2$**	**Interrupción $_3$**	**Comunicación de las condiciones legales y operativas $_4$**	**Autenticación$_5$**	**Plan de continuidad$_6$**
		Entidad	**Proveedor**					
Cajeros automáticos								
Puntos de Venta								
(e-banking).								
Banca Móvil (m-Banking)$_7$								
Otros, especifique								

Notas:

1 S= SI provee este servicio N= no provee este servicio.

2 Debe indicarse si el servicio opera en un esquema de proceso en tiempo real y conexión en línea directa con el computador que administra la red y la base de datos que opera.

3 En caso de interrupción, indique si el dispositivo o servicio queda fuera de servicio para todo tipo de transacciones hasta la normalización del proceso.

4 Indicar que medio utiliza la entidad para establecer y comunicar a sus clientes las condiciones legales y operativas bajo las cuales se brindará el servicio financiero, por ejemplo mediante contrato de adhesión o publicación de reglamentos.

5 Indicar las medidas de autenticación que utilizan para verificar la identidad de cada uno de los usuarios a los que preste sus servicios, así como los tipos de servicios de operaciones por Internet que cada uno de ellos tiene autorizado realizar.

6 Indicar si la entidad cuenta con un plan específico de continuidad del servicio.

7 Corresponde a transacciones cursadas por medio de dispositivos móviles, que utilicen comunicaciones de telefonía celular o de redes inalámbricas[174].

Se hace de nuevo la observación de la necesidad de un marco legal que marque las pautas relativas a la Banca por Internet y en especial a las medidas de seguridad mínimas con las que cada entidad debe contar. Como se mencionó supra, una buena opción sería el implementar un reglamento de la SUGEF en el que se indiquen una serie de mínimos de seguridad con la que toda entidad que quiera brindar el servicio de Banca por Internet deba contar, y que de ahí en adelante pueda ampliar sus posibilidades si lo

[174] Resolución del Superintendente SUGEF-R-839-2009. Superintendencia General de Entidades Financieras. Despacho del Superintendente General de Entidades Financieras, a las 9:40 horas del 06 de marzo de 2009.

desea, pero que incluya un parámetro mínimo en procura de la protección del consumidor y además para asegurar la relación entre éste y la entidad.

ii. Tecnologías:

A partir de los fraudes informáticos contra los clientes bancarios, los bancos decidieron implementar una serie de mecanismos de seguridad que funcionan como un segundo mecanismo de autenticación para el usuario. Es decir, además de la tradicional identificación a través de cédula y contraseña, se solicita que se inserten una serie de datos adicionales, generalmente una serie numérica aleatoria y desechable una vez utilizada.

Así, se inicia la utilización de Tokens, claves aleatorias, tarjetas dinámicas, teclados virtuales, listas de favoritos, entre otros, como medios que brinden mayor seguridad a los consumidores. Cada uno ha sido desarrollado en forma independiente por los bancos, pues como ya se indicó, no existe una regulación que determine el tipo de tecnología mínima por implementar.

Los Tokens, por ejemplo, funcionan a través de un dispositivo, que en el caso del Banco Nacional se ofrece a través de un llavero o una tarjeta, y también se puede colocar en el celular. A continuación se explica su funcionamiento:

> *"Es una plataforma que está sincronizada con un servidor principal y el periódicamente está dando un número aleatorio entonces la persona lo que hace con este token es que lo porta y dentro de los parámetros de autenticación que se solicitan se va a pedir el número que el token genera la persona lo digita y ahí entra en el proceso de autenticación, esto lo que hace es disminuir que al ser un parámetro variante en el tiempo se mantiene 5 ó 10 segundos elimina el hecho de que tal vez cuando son sólo los parámetros de la tarjeta o los parámetros de la cédula son muy fáciles de obtener, muy manipulables, en cambio con este método ni siquiera el mismo usuario sabe a ciencia cierta cuál es su clave de acceso."* [175]

En el caso de las tarjetas dinámicas, su utilización es mucho más simple, pues los datos que deben insertarse no se generan de manera automática, sino que resultan de una combinación de dígitos que vienen en una tarjeta portable.

[175] ALVARADO, Max (2009). Ingeniero en Sistemas. Entrevista en CISCO Systems, Plaza Roble. 06 de octubre de 2009.

Los teclados virtuales buscan eliminar los fraudes a través de key loggers pues los datos de las contraseñas no son digitados directamente en el teclado, sino que a través de una aplicación se crea un teclado virtual, de modo que aparece reflejado en la página y ahí es donde, con el mouse, se introduce la contraseña.

Todos estos dispositivos requieren una adecuada capacitación y la debida comprensión de los consumidores, ya que si se quiere una banca que sea ampliamente difundida y que rompa la brecha digital debe tomarse en cuenta el desconocimiento que la mayoría de la población tiene en materia de informática y sobretodo en cuanto a tecnología y seguridad. Es deber de los bancos informar ampliamente al consumidor, darle todas las posibilidades con las que cuenta de manera clara, comprensible y asegurarse que haya realmente comprendido el fondo de la situación, sin que se dé por un hecho que se comprende una tecnología de avanzada por una firma en un papel o un click en un sitio web.

Es cierto que el cliente tiene responsabilidades, pero para que las asuma correctamente es estrictamente necesario que comprenda que las tiene, que sepa que puede, debe y no debe hacer. Todo vacío en la comprensión del sistema genera un riesgo, que evidentemente perjudica al cliente y que debe ser subsanado por el banco cumpliendo con su deber de información.

Como ha sido con razón afirmado por los funcionarios bancarios y expertos en seguridad, de nada vale tener el sistema más avanzado de seguridad, la última tecnología, si el cliente no colabora con sus responsabilidades y cumple su parte. Pero también es cierto que para que el cliente efectivamente cumpla con sus obligaciones debe primeramente conocerlas, entenderlas, tener claro su papel en la contratación. Si no existe claridad no puede esperarse un comportamiento determinado, máxime cuando son temas especializados y requieren términos claros, entendibles y simples.

De aquí se deriva la tarea de concientización de los Bancos, que deben garantizar la adecuada difusión de la información, buscando un sistema más personalizado y claro, pues parte de los sucesos que se dan son por desconocimiento, por falta de información y el cambio no se ha dado aún. Existe aún un profundo desconocimiento por parte del usuario, que día a día utiliza los servicios por Internet de los bancos bajo el riesgo de perder sus activos.

La labor del banco no puede limitarse a poner a disposición de los clientes los mecanismos y dejar a su propia iniciativa el informarse, piénsese además en la tecnología que viene en camino con la firma digital, que requiere aún mayor diligencia por parte del usuario y un conocimiento mucho más técnico. Parte de la evaluación del riesgo y su

correlativa medida de disminución es valorar al cliente, actor principal en la relación, y darse a la tarea de informarlo y de constatar su comprensión efectiva. No debe darse por sentado que quien firma un contrato ya comprendió a cabalidad todos sus términos, porque se ha demostrado en experiencias propias y ajenas que no es así. De ahí han nacido las legislaciones para proteger al consumidor, que es la parte débil de la relación. El banco debe proteger también a sus clientes, eso es realmente una ideología de conciencia social, pero sobretodo una medida indispensable si pretende mantenerse en el mercado, pues depende directamente de la satisfacción de éste.

CAPÍTULO TERCERO

Costa Rica ante los Delitos Informáticos en la Banca por Internet

SECCIÓN I

GENERALIDADES DEL DERECHO DEL CONSUMIDOR

"Consumidores, por definición, nos incluye a todos, es el grupo más grande de la economía, que afecta y que está afectado por casi todas las decisiones públicas y privadas,… es el único grupo importante en la economía que no está organizado de manera efectiva, y cuyos intereses muy a menudo no son escuchados."[176]

[176] Discurso dado a los ciudadanos estadounidenses por el Presidente John F. Kennedy el 15 de marzo de 1962. Citado por SALAZAR SOLÓRZANO, Randall (S.F.). La Tutela Constitucional del consumidor. Instituto de Investigaciones Jurídicas, Facultad de Derecho de la Universidad de Costa Rica.<http://www.iij.derecho.ucr.ac.cr/archivos/documentacion/derecho%20del%20consumidor/La%20Tutela%20Constitucional%20del%20Consumidor.pdf> (2009)[Visita realizada el 10/02/10].

Con el crecimiento del comercio y de las distintas formas para realizar intercambio de bienes y servicios se desarrolla una preocupación por la protección del consumidor participante de estas relaciones comerciales. Con el fin de equilibrar la relación entre consumidor y productor se elaboran una serie de leyes y reglamentos a nivel internacional que poco a poco van permeando la legislación particular de cada país.

Asimismo, el derecho del consumidor empieza a abarcar distintos campos en los que encajan los conceptos de consumidor y en los que se visualiza una necesidad de protección de sus intereses. Se perfila entonces, que es menester brindarle protección al usuario de servicios dentro del comercio electrónico, entendiéndolo como la parte débil de la relación y vulnerable ante un marco poco regulado.

Las Naciones Unidas promulgan el 9 de abril de 1985 un instrumento internacional para la protección del consumidor, a través de las Directrices para la Protección al Consumidor, aprobadas por la Asamblea General de las Naciones Unidas 39/248. Estas directrices sirven a los gobiernos como base para formular una política de protección al consumidor de acuerdo con las circunstancias económicas, sociales y ecológicas de cada país y subsanar desequilibrios. En Costa Rica se tomó la declaración 39/248 de las

Naciones Unidas como marco para crear la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

Dentro de las necesidades legítimas que las Directrices procuran atender se encuentran las siguientes:

a) La protección de los consumidores frente a los riesgos para su salud y su seguridad.

b) La promoción y protección de los intereses económicos de los consumidores.

c) El acceso de los consumidores a una información adecuada que les permita hacer elecciones bien fundadas conforme a los deseos y necesidades de cada cual.

d) La educación del consumidor, incluida la educación sobre la repercusión ambiental social y económica que tienen las elecciones del consumidor.

e) La posibilidad de compensación efectiva al consumidor.

f) La libertad de constituir grupos u otras organizaciones pertinentes de consumidores y la oportunidad para esas organizaciones de hacer oír sus opiniones en los procesos de adopción de decisiones que las afecten.

g) La promoción de modalidades sostenibles de consumo.

Se tiene como consumidor a cualquier persona ya sea física o jurídica a la que le son suministrados bienes y servicios para su uso particular. Este concepto abarca cada día más situaciones pues constantemente se crean medios y productos para consumir, con lo que se ve aumentada la posibilidad de inversión de un consumidor en diversos productos que se encuentran disponibles en el mercado, aunado a las facilidades que cada día se le presentan para hacer posible ese consumo.

Dadas estas condiciones y la explosión del consumo en la actualidad, lo que aprovechan los productores para generar cada día más fuentes de ingreso, es que se comienza a regular y proteger la posición del consumidor frente a la del empresario o productor, tratando de crear relaciones más equitativas y justas. El productor es quien realmente posee la información completa del producto, y en ese tanto es quien debe informarle debidamente al consumidor las características, beneficios y riesgos que su producto posee.

El consumidor conoce el producto ofrecido gracias a la oferta que el productor que le hace, guía su decisión de consumo en ese sentido, es por ello que la información brindada debe ser veraz, completa, entendible. En relación con lo anterior, se justifica el porqué es el empresario o productor quien tiene el poder; la respuesta es simple: es quien maneja la información, quien sabe del producto y quien lo promociona. Por ello, debe asegurársele al consumidor que va a recibir el producto que se le ofrece, a través del equilibrio de posiciones mediante reglas que obliguen al productor a ser claro y preciso con la información que brinda. De ahí surge la necesidad de proteger al consumidor frente a posibles abusos de poder por parte del productor.

Teniendo clara esta desigual relación, es que nace el Derecho del consumidor, con la finalidad de equilibrar la relación entre consumidor y productor. Se pretende regular las relaciones de mercado para lograr una situación justa entre los actores de la cadena de consumo, sin que existan abusos por parte de los productores en menoscabo de los derechos del consumidor.

Costa Rica se ha sumado a la tendencia de protección de los derechos del consumidor y ello es visible, por ejemplo, en los criterios esgrimidos por la Sala Constitucional con

respecto a la necesidad de dicha protección, así se puede extraer de la sentencia 1441-92, en la que se indica:

> "*es notorio que el consumidor se encuentra en el extremo de la cadena formada por la producción, distribución y comercialización de los bienes de consumo que requiere adquirir para su satisfacción personal y su participación en este proceso, no responde a razones técnicas ni profesionales, sino en la celebración constante de contratos a título personal. Por ello su relación, en esa secuencia comercial es de inferioridad y requiere de una especial protección frente a los proveedores de los bienes y servicios, a los efectos que de previo a externar su consentimiento contractual cuente con todos los elementos de juicio necesarios, que le permitan expresarlo con toda libertad y ello implica el conocimiento cabal de los bienes y servicios ofrecidos. Van incluidos por lo expresado, en una mezcla armónica, varios principios constitucionales, como la preocupación estatal a favor de los más amplios sectores de la población cuando actúan como consumidores, la reafirmación de la libertad individual al facilitar a los particulares la libre disposición del patrimonio con el concurso del mayor conocimiento posible del bien o servicio a adquirir, la protección de la salud cuando esté involucrada, el ordenamiento y la sistematización de las relaciones recíprocas entre los interesados, la*

homologación de las prácticas comerciales internacionales al sistema interno y en fin, la mayor protección del funcionamiento del habitante en los medios de subsistencia..."[177]

Como resultado de lo anterior, se promulga el 19 de diciembre de 1994 la Ley No. 7472 de Promoción, Competencia y Defensa Efectiva del Consumidor. El objetivo de esta ley es proteger, efectivamente, los derechos y los intereses legítimos del consumidor, la tutela y la promoción del proceso de competencia y libre concurrencia, mediante la prevención, la prohibición de monopolios, las prácticas monopolísticas y otras restricciones al funcionamiento eficiente del mercado y la eliminación de las regulaciones innecesarias para las actividades económicas[178].

También, la Constitución Política protege al consumidor en su artículo 46, que fue objeto de modificación en el año 1996 mediante Ley No. 7607, introduciéndose en él un nuevo derecho económico justo al lado de la libertad de empresa y como delimitador de ésta: la protección del consumidor[179]. Así queda manifestado en el párrafo final del mencionado artículo:

[177] Voto N° 1441-92 de la Sala Constitucional de la Corte Suprema de Justicia, de las 15:45 hrs. del 2 de junio de 1992
[178] Ley 7472 de Promoción de la Competencia y Defensa Efectiva del Consumidor, Artículo 1.
[179] Sala Primera de la Corte Suprema de Justicia. Sentencia 295-07 de las diez horas cuarenta y cinco minutos del veintiséis de abril del dos mil siete.

"Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos. La ley regulará esas materias."

Quedan de modo general establecidos los derechos básicos con los que cuenta el consumidor en Costa Rica, estos se desarrollan de modo específico en la Ley No. 7472 y en normativa internacional, por ejemplo, en las Directrices de la ONU y en reglamentos de Asociaciones y Organizaciones de Derechos del Consumidor. Para la Organización de Consumidores Internacionales (Consumers International), todo consumidor cuenta con ocho derechos básicos, a saber:

1. "Derecho a la satisfacción de necesidades básicas: tener acceso a bienes y servicios básicos esenciales; adecuados alimentos, ropa, vivienda, atención de salud, educación, servicios públicos, agua y saneamiento.

2. Derecho a la seguridad: ser protegido/a contra productos, procesos de producción y servicios peligrosos para la salud o la vida.

3. Derecho a ser informado/a: acceder a los datos necesarios para poder hacer elecciones informadas y ser protegido/a contra publicidad y etiquetados deshonestos o engañosos.

4. Derecho a elegir: poder elegir entre un rango de productos y servicios, ofrecidos a precios competitivos con la garantía de seguridad y buena calidad.

5. Derecho a ser escuchados/as: los intereses de los consumidores deben estar representados en la aplicación de políticas gubernamentales y en el desarrollo de productos y servicios.

6. Derecho a la reparación: recibir resoluciones justas por demandas justas, incluyendo la compensación por bienes mal hechos o servicios insatisfactorios.

7. Derecho a la educación como consumidores: adquirir conocimientos y habilidades necesarias para estar informados y hacer elecciones apropiadas sobre bienes y servicios y, al mismo tiempo, estar conscientes de los derechos y responsabilidades básicas de los consumidores y saber cómo actuar sobre ellos.

8. Derecho a un ambiente saludable: vivir y trabajar en un ambiente que no amenace el bienestar de las generaciones presentes ni futuras."[180]

Por su parte, la Ley de Defensa Efectiva del Consumidor (Ley 7472) establece en su artículo 32 los derechos del consumidor, calificándolos como fundamentales e irrenunciables:

a) La protección contra los riesgos que puedan afectar su salud, su seguridad y el medio ambiente.
b) La protección de sus legítimos intereses económicos y sociales.
c) El acceso a una información, veraz y oportuna, sobre los diferentes bienes y servicios, con especificación correcta de cantidad, características, composición, calidad y precio.
d) La educación y la divulgación sobre el consumo adecuado de bienes o servicios, que aseguren la libertad de escogencia y la igualdad en la contratación.
e) La protección administrativa y judicial contra la publicidad engañosa, las prácticas y las cláusulas abusivas, así como los métodos comerciales desleales o que restrinjan la libre elección.

[180] Consumers International es una Federación mundial de organizaciones de consumidores fundada en 1960, con más de 220 organizaciones asociadas en 115 países

f) Mecanismos efectivos de acceso para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a prevenir adecuadamente, sancionar y reparar con prontitud la lesión de estos, según corresponda.

g) Recibir el apoyo del Estado para formar grupos y organizaciones de consumidores y la oportunidad de que sus opiniones sean escuchadas en los procesos de decisión que les afecten.

(Así modificada su numeración por el artículo 80 de la ley N° 8343 de 27 de diciembre del 2002, Ley de Contingencia Fiscal, que lo pasó del 29 al 32)

Del mismo modo, la mencionada Ley establece en su numeral 34 las obligaciones que tienen los productores o comerciantes de bienes y servicios, quienes deben acatar las disposiciones en amparo del consumidor en sus contrataciones. Para la presente investigación son de particular interés los incisos b), c), d) y o).

> *"b) Informar suficientemente al consumidor, en español y de manera clara y veraz, acerca de los elementos que incidan en forma directa sobre su decisión de consumo. Debe enterarlo de la naturaleza, la composición, el contenido, el peso, cuando corresponda, las características de los bienes y servicios, el precio de contado en el empaque, el recipiente, el envase o la etiqueta del producto y la góndola o el anaquel del establecimiento comercial, así como*

de cualquier otro dato determinante. Si se trata de productos orgánicos, esta condición deberá indicarse en un lugar visible. Además, la etiqueta del producto deberá indicar cuál es el ente certificador. De acuerdo con lo dispuesto en el Reglamento de la presente Ley, cuando el producto que se vende o el servicio que se presta se pague al crédito, deben indicarse, siempre en forma visible, el plazo, la tasa de interés anual sobre saldos, la base, las comisiones y la persona, física o jurídica, que brinda el financiamiento, si es un tercero.

(Así reformado el inciso anterior mediante el artículo 40 de la ley N° 8591 del 28 de junio del 2007).

c) Ofrecer, promocionar o publicitar los bienes y servicios de acuerdo con lo establecido en el artículo 34 de esta Ley. (Por modificación el artículo 34 es actualmente el 37)

d) Suministrar, a los consumidores, las instrucciones para utilizar adecuadamente los artículos e informar sobre los riesgos que entrañe el uso al que se destinan o el normalmente previsible para su salud, su seguridad y el medio ambiente.

o) Apegarse a la equidad, los buenos usos mercantiles y a la ley, en su trato con los consumidores.

Toda información, publicidad u oferta al público de bienes ofrecidos o servicios por prestar, transmitida por cualquier medio o forma de comunicación, vincula al productor que la transmite, la utiliza o la ordena y forma parte del contrato.

El incumplimiento de alguna de las obligaciones enumeradas en este artículo, faculta al interesado para acudir a la Comisión nacional del consumidor creada en esta Ley, o a los órganos jurisdiccionales competentes y para hacer valer sus derechos, en los términos que señala el artículo 43(*)de la presente Ley.
(Así modificada su numeración por el artículo 80 de la ley N° 8343 de 27 de diciembre del 2002, Ley de Contingencia Fiscal, que lo pasó del 31 al 34)
(*)(Actualmente corresponde al artículo 46)"

Como puede apreciarse en el último párrafo del citado artículo, se faculta al consumidor a entablar un procedimiento en caso de incumplimiento por parte del productor de alguna de estas obligaciones. Se refiere al artículo 46 para efectuar la

reclamación, y éste indica que puede realizarse por vía administrativa o por vía judicial, sin que se excluyan entre sí, excepto si se opta por la vía judicial. Sin embargo, la ley excluye de su competencia la anulación de cláusulas abusivas en los contratos de adhesión y el resarcimiento de daños y perjuicios, ambos deben reclamarse por la vía judicial.

En la ley 7472, asimismo, se crea y da competencia a la Comisión Nacional del Consumidor para que actúe como órgano de máxima desconcentración adscrita al Ministerio de Economía, Industria y Comercio, velando por el cumplimiento de lo establecido en la ley y demás normas que garanticen la defensa efectiva del consumidor. De igual forma, la mencionada ley fomenta la creación de organizaciones de consumidores y les da la legitimación procesal, de acuerdo al artículo 54, para iniciar como parte o intervenir, en calidad de coadyuvantes, en los procedimientos ante la Comisión nacional del consumidor y ante los tribunales de justicia, en defensa de los derechos y los intereses legítimos de sus asociados. La coadyuvancia se rige por lo establecido en la Ley General de la Administración Pública y en el Código Procesal Civil.

Es por ello, que empiezan a surgir en Costa Rica asociaciones y organizaciones con el fin de proteger los derechos de los consumidores. Nacen entre ellas la Organización de

Consumidores de Costa Rica y la Asociación de Consumidores Libres (ACL). La Organización de Consumidores de Costa Rica tiene el siguiente fin:

> *"Consumidores de Costa Rica, nace con el afán de profesionalizar el trabajo de las organizaciones de consumidores en el país, de manera que se una a otros esfuerzos realizados en esta materia por precursores institucionales y privados, con el principal eje diferenciador de anteponer un modelo de solidaridad entre consumidores, sector privado y el Estado, de manera que los intereses de todos, encuentren el equilibrio necesario para que el comercio y la prestación de los servicios públicos se de bajo los principios de la información, solidaridad y justicia para los consumidores."*[181]

A su vez la Asociación de Consumidores Libres (ACL) tiene como objetivo principal:

> *"Defender a ultranza los derechos de los consumidores frente al Estado y los productores e industriales. Lo que significa el derecho a comerciar (comprar, vender, importar, exportar, intercambiar, regalar, recibir regalos, etc. sin ninguna restricción) el cual incluye el derecho a adquirir bienes y servicios de*

[181]Consumidores de Costa Rica (2009). http://www.consumidoresdecostarica.org/informacion_general.html. [Consulta del 02 de noviembre del 2009].

cualquier oferente sin importar su raza, religión, nacionalidad, afinidad sexual y cualquier otra característica."[182]

Dentro de sus actividades, la ACL indica el iniciar o intervenir en calidad de coadyuvantes procedimientos ante la Sala Constitucional y los tribunales de justicia para defender los derechos e intereses legítimos de los consumidores. Es así como la ACL se dio a la tarea de buscar a usuarios de la banca afectados por delitos informáticos e iniciar junto a ellos un proceso colectivo por intereses colectivos y difusos, tema que será analizado más adelante.

[182] Asociación de Consumidores Libres (2009). http://www.consumidoreslibres.org/index.htm. [Consulta del 02 de noviembre del 2009].

SECCIÓN II

EL CONSUMIDOR, LOS BANCOS Y EL CONFLICTO

2.1 POSICIÓN DEL CONSUMIDOR

El servicio de banca por Internet se encuentra disponible de manera gratuita y abierta para toda aquella persona afiliada a un banco al cual éste le brinde la opción. Como requisitos se solicitan, primero y de forma indispensable, tener una cuenta con el banco, ya sea de crédito o de débito; además, de modo particular para cada entidad bancaria, se han elaborado contratos para el servicio de *Internet Banking* que deben ser aceptados por el usuario para así poder hacer uso de este servicio.

La banca, tanto privada como estatal, ha manejado de diversas maneras el tema de la aceptación o manifestación de la voluntad en cuanto a las cláusulas del contrato para la Banca por Internet. Tal y como se analizó con anterioridad, en algunos casos la entidad de manera física entrega el contrato y solicita que éste sea firmado

con una firma manuscrita; otros bancos, en cambio, incluyen en la página de Internet de la entidad el Reglamento de servicios de Banca por Internet y el cliente sólo debe pulsar con el ratón un espacio en donde indica que leyó y está de acuerdo con los términos del mismo. Adicionalmente incluye datos de su tarjeta, tales como el número, la fecha de vencimiento y el PIN. Una vez finalizado este proceso, el usuario se encuentra habilitado para realizar todas las posibilidades que pone a disposición la banca de su preferencia.

En el presente trabajo se realizó una encuesta representativa a 103 personas, todas ellas mayores de edad, de distintos estratos sociales, de ambos sexos, todos usuarios del servicio de banca por Internet. Los datos obtenidos sirven para ejemplificar el comportamiento general de la población consumidora de este tipo de servicio. Se obtuvieron datos que ayudan a entender las necesidades de esta población, sus mayores deficiencias y el esquema de conceptos manejados.

Así, es de particular interés el conocer, con la muestra obtenida, cuál es el porcentaje de usuarios pertenecientes a la Banca Estatal y cuáles son clientes de la Banca Privada. Lo anterior, pues los casos por fraudes informáticos llevados a la sede judicial han sido únicamente los correspondientes a la Banca Estatal. No obstante, no

debe interpretarse que no han existido casos de delitos informáticos en la Banca Privada, la explicación es sencilla: todos los casos se han conciliado.

Volviendo al punto de atención, según el muestreo, un 64% de los encuestados utilizan la banca estatal, un 9% utilizan la banca privada y un 27% ambas. Este resultado, visto puramente desde una perspectiva matemática, explica el porqué la banca estatal se ha visto estadísticamente más afectada que la banca privada. La banca que posee más usuarios es la que sirve como el blanco más atractivo para cometer delitos informáticos. Este dato fue confirmado por las autoridades bancarias que fueron entrevistadas en el desarrollo de la investigación del presente trabajo, indicando que los números son en su mayoría desfavorables para la banca estatal, sobre todo para el Banco Nacional, pues es quien posee una mayor cartera de clientes, tanto en el país como en el extranjero.

En la encuesta aplicada, se dio a relucir que los clientes de Banca por Internet utilizan este servicio principalmente para efectuar pagos de servicios públicos, así como para revisar sus estados de cuenta, realizar transacciones entre cuentas y a través del servicio SINPE, entre otros. Estas transacciones son realizadas en un 26% en sus casas de habitación, un 11% las realizan en sus trabajos, en la casa y el trabajo un 58%, en el trabajo y otros un 3%, en la casa y otros un 2% y un 0% en Cafés Internet.

Este resultado es particularmente interesante, pues muestra que existe una conciencia generalizada de realizar las transacciones en los lugares que son aconsejados como los idóneos para realizar las operaciones por Internet. Llama la atención que un 0% de los encuestados realicen sus trámites electrónicos en Cafés Internet, a pesar de la publicidad que algunas agencias bancarias realizan al respecto, tal como fue expuesto con anterioridad en el Capítulo II, sección I cuando se tocó el tema de la Banca por Internet o *Internet Banking*, al hacer alusión a la publicidad que el Banco Nacional incluye en su página de Internet[183], pues se enumera dentro de las ventajas del servicio de *Internet Banking* el realizar las operaciones desde un Café Internet, a pesar de que los expertos en seguridad, otras instituciones bancarias, jueces de la República, entre otras múltiples fuentes, han determinado que estos sitios no son recomendados para ejecutar transacciones electrónicas.

[183] Ya se realizó una nota al pie al respecto, en diversas ocasiones durante el año 2009 y principios del 2010 se revisó el link en el que se encuentra esta información y la misma se mantiene sin ninguna modificación. En la página del Banco Nacional se encuentra una sección denominada Antiphishing, en la que se da una serie de advertencias y consejos a los clientes, sin embargo se anota únicamente que si se realizan transacciones desde un Café Internet debe asegurarse que éste cuente con los requerimientos de seguridad necesarios, que no son detallados para el cliente, por lo tanto se continúa en la actitud de promocionar un medio que ha sido determinado por los mismos personeros del banco como no apto para realizar transacciones bancarias; lo mismo debe apuntarse en cuanto a el Banco de Costa Rica, que incluye la opción del Internet café como una de los medios para acceder a la Banca por Internet. La crítica recae en que los bancos están indicando que es posible realizar las transacciones en Cafés Internet si se revisa la seguridad con lo que éstos cuentan, sin embargo no indican cuáles son esos requisitos que debe incluir una red pública, los cuidados particulares que haya que tener ni las advertencias de seguridad necesarias para que el cliente, con suficiente conocimiento, pueda distinguir entre un lugar seguro y otro que no lo es, así como los elementos básicos con los que debe contar el equipo por utilizar.

A pesar de este tipo de información, los clientes encuestados mantienen un comportamiento atinente a las políticas de seguridad que se han dado, aún y con la deficiencia notable de información o incluso mal información al respecto. Este comportamiento no puede generalizarse, pues sí existen casos reportados en los cuales los clientes utilizan los Internet Cafés para realizar sus operaciones bancarias por Internet, por lo que no debe excluirse esta opción.

También es menester enfatizar que la mayoría de los encuestados utilizan su casa de habitación o su lugar de trabajo como su lugar predilecto para accesar a su cuenta bancaria. El resultado obtenido debe contrastarse con varias de las preguntas formuladas, a saber, si se utiliza un antivirus, si éste fue comprado o descargado gratuitamente, si se sabe distinguir una página segura de otra que no la es, entre otras, que serán analizadas a continuación.

Como primer punto se procede a analizar, de acuerdo con las respuestas obtenidas, si los usuarios encuestados tienen algún cuidado especial a la hora de realizar transacciones por Internet. Los datos son los siguientes, un 83% del total aseguran tener cuidados especiales, mientras un 17% indica que no tienen ningún cuidado en particular. De ahí que a pesar de no realizar las transacciones en un Café

Internet, a la hora de utilizar el servicio de Banca *Online* existe un porcentaje que no se preocupa por tener cuidado alguno con sus accesos a las páginas bancarias.

Un segundo punto por analizar corresponde a si los encuestados se aseguran de utilizar dispositivos de seguridad en la computadora que utilizan para sus accesos a Internet. Un 87,4% indicó que sí, mientras que un 12,6% contestó negativamente. Al grupo de encuestados que contestó que sí se aseguran de contar con dispositivos de seguridad, se les preguntó sobre cuáles dispositivos se aseguraba tener, los resultados arrojaron que un 94,44% de ese total se preocupa por tener antivirus, un 62,22% cuentan con Anti-Spyware, un 57,78% se asegura de tener Firewall y un 6,67% poseen otros dispositivos. En conclusión, los encuestados que sí se preocupan por los dispositivos de seguridad con los que cuenta la computadora que utilizan para sus movimientos y accesos en general a Internet, lo hacen principalmente en cuanto al Antivirus.

En un tercer aspecto, se analiza de acuerdo al porcentaje anterior de encuestados que se preocupan por tener dispositivos de seguridad, en específico el antivirus, si además de poseerlo se encuentran pendientes de su actualización. Un 71% contestó afirmativamente, y un 29% contestó de forma negativa. Este resultado permite indicar que a pesar de que la mayoría de encuestados afirman tener un

antivirus, existe un porcentaje que no lo tiene actualizado, o por lo menos que no se preocupa de su debida actualización. Debe recordarse que dentro de las recomendaciones de los expertos en seguridad se encuentra el hecho de tener un antivirus actualizado, pues los virus constantemente están mutando o se están creando nuevos, por lo que las bases de datos de virus se modifican de forma continua para encontrar debidamente protegido contra éstos. Así, no basta el hecho de tener un antivirus, éste debe estarse en constante actualización para darle un óptimo empleo.

Aunado a lo anterior, se preguntó a este mismo grupo encuestado si realizaba revisiones a su computadora para comprobar si ésta se encuentra libre de virus y amenazas. Los datos obtenidos son muy similares a los recién vistos, ya que un 72% contestó que sí realiza revisiones, en contraposición a un 28% que contestó que no. Valga la anotación anterior para este resultado, ya que igualmente es necesario realizar con cierta frecuencia análisis a la computadora, con el fin de asegurarse que la misma se encuentre libre de cualquier amenaza y así tener un mayor grado de seguridad con lo que se accedería de modo correcto a sitios de Internet, especialmente a las páginas bancarias.

En otro punto, se preguntó si se sabe o no distinguir un sitio en Internet catalogado como seguro de otro que no lo es. Los resultados expresan que un 51,5%

de los encuestados saben distinguir un sitio seguro, mientras que un 48,5% contestó que no sabe realizar esa distinción. Estos porcentajes resultan sumamente interesantes, pues contrastan mucho con la pregunta relacionada al cuidado especial que los usuarios encuestados indican tener cuando ingresan a la red. Parte de los cuidados que los bancos recomiendan tener, es precisamente el lograr identificar que el sitio es seguro constatando que la página de acceso sea la de la entidad bancaria, y esa certeza se tiene cuando se revisa que, por ejemplo, el nombre de dominio coincida con el de la página del banco, que la página haya sido desarrollada bajo el protocolo SSL (recordando lo que anteriormente se vio al respecto), que exista un certificado de autenticidad representado por el candado que aparece en la parte inferior derecha de la barra de dirección del navegador Web. Estos puntos ha revisar han sido indicados en las páginas de los bancos, ya sea en información sobre seguridad o en demos que han puesto para que sean revisados por los clientes.

De ahí que existe, según los datos obtenidos, un vacío en los conocimientos de los clientes de la banca por Internet sobre la seguridad de las páginas que visitan, ya que casi la mitad de los encuestados expresa no poder distinguir un sitio catalogado como seguro de otro que no lo es. Esta situación implica un riesgo para el cliente, que con esta deficiencia puede ingresar sin saberlo a sitios no seguros y ser víctima de un fraude informático.

En otro punto, se preguntó a los usuarios encuestados si éstos utilizaban la opción de “recordar contraseña” en los sitios que utilizan en Internet. Los resultados dejan ver que un 21% de ellos sí emplean esta opción, mientras que un 79% no lo hace. Esta pregunta se realizó con el fin de determinar cuántas personas cumplen con la recomendación de no recordar contraseñas en su computadora y cuantas no. El peligro que se corre utilizando esta posibilidad, es que si se instala un Spyware o Malware dentro de la computadora se pueda detectar por los delincuentes cibernéticos las contraseñas que han sido guardadas e ingresar a dichas páginas suplantando la identidad de los usuarios.

En la encuesta aplicada, se quiso indagar sobre la participación bancaria en el proceso de capacitación de los clientes sobre la seguridad, riesgos y medidas que deben tomar los clientes a la hora de ingresar a la página en línea de los bancos. Para este particular, se hizo la pregunta de si se ha recibido algún tipo de capacitación por parte de los bancos para el uso de Banca por Internet. El porcentaje de encuestados que manifestaron que sí han recibido capacitación es de un 20%, en oposición a un 80% que indicó que no.

En la presente investigación, se propone que las entidades bancarias capaciten directa y efectivamente a sus usuarios. Esto disminuye el riesgo por desconocimiento, permite una adecuada información al cliente sobre el servicio y ayudaría a bajar los índices de fraudes por engaño a los usuarios bancarios. Esta capacitación, según se plantea en este trabajo, debe ser un requisito indispensable para que se pueda ingresar al servicio de Banca por Internet, es decir, debe cumplirse con el requerimiento de la capacitación para que el usuario pueda hacer uso del servicio de *Internet Banking.*

Una alternativa de capacitación es utilizar las presentaciones o demos que tienen en las páginas bancarias, por ejemplo la del BAC San José, el Banco de Costa Rica o el Banco Nacional, con las modificaciones que sean necesarias para complementar la información y colocarlas como requisito indispensable a completar antes de ingresar por primera vez al sitio. Esta capacitación debe contener evaluaciones que comprueben la adecuada comprensión de la información por parte de los consumidores.

De esta manera, puede corroborarse que el cliente obtuvo la información necesaria para su seguridad por parte de la entidad que tiene la obligación de suministrársela, en adecuado cumplimiento del derecho de información que éste

posee y además el banco cumple con su deber de concientización, considerado para efectos de esta investigación como un elemento indispensable dentro de la seguridad que debe poseer, con lo que incluso se asegura un argumento a favor al respecto de sus actuaciones al capacitar debidamente a los usuarios de sus servicios.

Pasando a otro punto, en una revisión de las páginas bancarias, tal y como acaba de señalarse se encontró con que la mayoría indica en sus páginas una serie de consejos de seguridad para el cliente, entre ellos demos o presentaciones interactivas para suministrar información al usuario sobre los cuidados que debe tener a la hora de accesar al servicio de banca por Internet. Estos consejos y demos son de acceso voluntario, es decir, el cliente decide si quiere verlos o no, sin que sean un requisito para ingresar al servicio brindado. Por esta razón, se hizo necesario conocer a través de la encuesta, cuántas personas han revisado estos consejos y/o demos; así, un 58% de los encuestados afirma haber revisado los consejos pero un 42% manifestaron que no lo han hecho.

Bajo este supuesto, puede concluirse que los demos a pesar de que son visitados por algunas personas, no representan, tal y como están diseñados, una opción efectiva de capacitación al cliente, pues es una gran cantidad de usuarios no revisan este tipo de recursos, sumando esto al hecho de que no se recibe una

capacitación personalizada del banco al cliente, con lo que se detecta un sector importante de usuarios con grandes deficiencias en la información, ya sea porque no le es suministrada o porque no se da a la tarea de revisarla. De nuevo se insiste en la necesidad de crear un mecanismo que efectivamente cumpla con el deber de información al cliente y que obligue al mismo a recibirla. La forma voluntaria no ha funcionado como debería, es por eso que para tener certeza al respecto, debe crearse una herramienta de uso obligatorio, por ejemplo, lo que se propone *supra*.

Continuando con el tema de verificación de conocimiento, se les preguntó a los usuarios si sabían el significado de los conceptos Phishing, Pharming, Troyanos, Spyware y Malware. Del total de los encuestados, quienes tenían posibilidad de indicar si conocían uno, varios o ninguno de esos conceptos, se logró recopilar que un 64,08% sabe qué es Phishing, un 14,56% tiene conocimiento acerca de Pharming, un 87,38% conoce sobre Troyanos, un 61,17% sobre Spyware y un 35,92% conoce de Malware. De acuerdo a estos resultados, los usuarios encuestados se encuentran más familiarizados con los conceptos Troyanos, Phishing y Spyware, en orden respectivo, lo que coincide con los tipos de delitos informáticos que mayor incidencia han tenido en casos relacionados con el tema en cuestión. Esto se debe, en mayor medida, ha que han sido las situaciones que se han visto más publicitadas, tanto por los bancos como por

distintos medios de comunicación, lo que ha generado un conocimiento social de dichos conceptos.

En medios de comunicación escritos y televisivos han sido expuestos en gran manera los casos de fraudes informáticos ocurridos, y generalmente se hace alusión al Phishing, por lo que la gente reconoce con mayor facilidad este tipo de delito informático[184].

Es también menester para esta investigación, saber si los bancos ofrecen algún dispositivo extra de seguridad además de la clave de acceso o contraseña. Con este fin, se preguntó en la encuesta a los usuarios si los bancos que utilizan les brindan ese tipo de dispositivos. Se obtuvo como resultado que un 70% de las entidades bancarias, tanto públicas como privadas ofrecen dispositivos extra, y un 30% no lo hace. Esta respuesta se relaciona con la que se obtuvo por la pregunta correspondiente a si el usuario que dispone de estas herramientas efectivamente las utiliza, encontrando que un 51% de los clientes bancarios sí utilizan los dispositivos, pero un 49% no lo hace.

Esto es factible pues algunos bancos, a pesar de ofrecer los dispositivos extra, permiten que se realicen ciertos movimientos sin necesidad de aportar los datos

[184] En la sección de anexos del presente trabajo se agrega una serie de noticias e informes sobre el tema, escogidos dentro de una gran variedad que se han originado al respecto.

correspondientes a esa herramienta adicional. De modo tal que, el usuario está posibilitado de realizar pagos de servicios públicos, pagos entre sus cuentas y tarjetas, entre otros, sin necesidad de aportar los datos de un dispositivo. Con lo anterior, puede evidenciarse un vacío, ya que si efectivamente se procura tener un mecanismo de autenticación adicional éste debería ser de uso obligatorio para todas y cada una de las transacciones o movimientos que se puedan realizar en la página, sino se permitiría un portillo para que una persona que obtiene los datos básicos solicitados pueda defraudar al consumidor de servicios bancarios por Internet.

Como última pregunta se solicitó a los encuestados realizar una evaluación de la seguridad que le ofrece el banco de su predilección. En cuanto a la Banca Estatal se obtuvo los siguientes resultados: Un 9,5% de los usuarios calificaron el servicio como excelente, un 40% como muy bueno, un 46,3% como bueno, un 4,2% como malo y un 0% como muy malo. Por otra parte, con respecto a la Banca Privada se obtuvo los siguientes resultados: un 5% de los encuestados calificó su servicio de banca por Internet como excelente, un 49% como muy buena, un 38% como buena, un 5% como mala y un 3% como muy mala.

En síntesis, realizando un perfil del consumidor de servicios de Banca por Internet, a través de la información obtenida en la encuesta, de las entrevistas

realizadas para esta investigación y de las noticias difundidas por los medios de comunicación nacional, puede decirse que éste se caracteriza por utilizar mayoritariamente la Banca Estatal. En términos generales posee algún tipo de conocimiento sobre los cuidados que deben tener en el equipo que utiliza para las transacciones y en los accesos que realiza a las páginas bancarias; estos conocimientos han sido adquiridos principalmente a través de canales externos, por ejemplo, los medios de comunicación, y en menor porcentaje han sido interiorizados a través de la capacitación de las entidades bancarias.

Además, a pesar de que una mayoría de los clientes asegura prestar cuidados especiales a la hora de ingresar a *Internet Banking*, lo cierto es que una vez que se le pregunta sobre recomendaciones básicas que se deben tomar para la utilización de este servicio los números cambian, y dejan entrever que dichos cuidados no son manifestados en la realidad.

La falta de información y la imprudencia que ésta genera son las principales problemáticas que el cliente presenta. Un usuario educado, capaz de reconocer engaños y trampas que se le presentan por parte de los delincuentes cibernéticos, implica un servicio más eficiente, una baja en los porcentajes de víctimas de este tipo de fraudes y una disminución en el riesgo del servicio. Es obligación del prestatario

cumplir con la adecuada información y asegurarse que el consumidor la haya comprendido adecuadamente, para que esté conciente de los riesgos que determinada actividad pueda conllevar y tome una decisión racional y con pleno conocimiento de todas las posibilidades que ésta le pueda generar.

Cierto es que la Teoría del Riesgo creado no permite que el banco se exima de responsabilidad si la actividad que presta genera un riesgo, pero es también cierto que éste se vería disminuido con políticas de información y concientización, como conjunto el tema de seguridad en donde no basta el sólo incluir herramientas tecnológicas, es necesario que se eduque al cliente, que se le informe y que éste utilice adecuadamente lo que se ha puesto a su disposición sin aumentar los riesgos por desconocimiento.

Los consumidores que se han visto afectados por los delitos informáticos han tenido varias alternativas para solucionar su conflicto, por un lado se encuentra la posibilidad de conciliar, siempre y cuando tanto el banco como el cliente se encuentren de acuerdo, este ha sido el panorama que ha regido en cuanto a la Banca Privada. Por otro lado se encuentra la opción, si no se resuelve en vía administrativa o en una conciliación, de acudir a los Tribunales de Justicia competentes. Esta opción es la que más han tomado los clientes de la Banca Estatal, pues como política bancaria en un inicio no se conciliaba (el Banco de Costa Rica ha empezado a utilizar la conciliación

como resolución del conflicto desde finales del 2009), y si no se resuelve en sede administrativa al cliente no le queda más opción que acudir a la sede judicial.

Los consumidores se encuentran facultados para acudir a los Tribunales con patrocinio letrado propio o bien representados por una Organización de Derechos del Consumidor. La Asociación de Consumidores Libres ha sido la principal impulsora de los derechos de los usuarios bancarios en sede judicial, y se ha encargado de representar a múltiples víctimas a través de un instituto novedoso y poco conocido en Costa Rica ,a saber, los Procesos Colectivos que serán analizados a continuación.

i. Los Procesos Colectivos en materia del consumidor

Los procesos colectivos o acciones colectivas pueden definirse como una acumulación de pretensiones de una variedad de afectados dentro de un solo proceso, con el fin de dotar de celeridad procesal a la resolución de los conflictos, además por motivos de economía procesal y de protección de las víctimas sobre todo en el tanto de que exista uniformidad en la resolución de la controversia. Así, en un solo proceso pueden existir múltiples víctimas representadas, sin necesidad de que cada una de ellas acuda de forma independiente a los Tribunales de Justicia.

La necesidad de establecer los procesos colectivos dentro de la legislación procesal costarricense, nace de la insuficiencia de los conceptos de derechos subjetivos e intereses legítimos como condicionantes de acceso a la justicia[185]. Con el establecimiento de los procesos colectivos se da un reconocimiento de los intereses supra individuales, tales como los intereses difusos, los colectivos y los individuales homogéneos.

Los intereses difusos son definidos como los intereses que no son determinados o determinables para una persona en particular, sino que funcionan para un colectivo que tiene una situación determinada. Así, son los intereses de una comunidad, de la sociedad. De hecho, una de sus características es precisamente el no pertenecer a una persona determinada o incluso a un grupo definido, sino que pertenecen a un grupo indeterminado de individuos. Es por ello que es supra individual, pues trasciende o excede al individuo, pero es ejercida por uno de los sujetos.

Además, doctrinariamente se ha indicado que esta colectividad se encuentra unida por una circunstancia de hecho común, un bien jurídico que les corresponde a todos, de modo tal que si el interés es satisfecho para uno lo es para todos, así como si

[185] ROJAS RIVERO, Adriana (2009). Procesos colectivos en el Código Procesal Contencioso Administrativo. IX Jornadas de AUSBANC Internacional: Nuevos Derechos Financieros del Siglo XXI. San José, Costa Rica. 02 de Octubre de 2009. [Ponencias recopiladas en Disco Compacto]

se sufre una lesión para uno se lesiona a todos. En los intereses difusos no existe un vínculo jurídico que una a los sujetos en una relación, ni tampoco una titularidad, únicamente son todos parte de una colectividad que ostenta un derecho que se ve lesionado o amenazado.

Son características de los intereses difusos[186]:

- No titularidad.
- Indisponibilidad.
- Indivisibilidad.
- Inapropiabilidad.

Por su parte, en los intereses colectivos, a diferencia de los intereses difusos, existe una relación jurídica base entre los interesados, o entre éstos y un tercero. Se trata de un grupo determinado o fácilmente determinable, con contornos definidos de forma más nítida. Se trata siempre de una colectividad, pero en esta situación este grupo de personas sí son identificables.

Se ha dicho doctrinariamente, que el interés difuso es el género y el interés colectivo una especie. Así se encuentra, por ejemplo la siguiente definición: "*En una primera*

[186] Ibídem.

aproximación podríamos considerar que el interés colectivo es una especificación del interés difuso. Pero el interés colectivo es a diferencia del difuso el de un grupo más o menos determinable de ciudadanos, perseguible de manera unificada, por tener dicho grupo unas características y aspiraciones sociales comunes."[187]

Por otro lado, se encuentran los denominados intereses individuales homogéneos, que son definidos de la siguiente manera:

> *"Los intereses individuales homogéneos, son aquellos que siendo particulares, pueden ser tratados procesalmente como colectivos, pues al existir condiciones idénticas se justifica su protección colectiva, por razones prácticas y de conveniencia. Pensemos en un accidente aéreo, por el cual mueren 200 personas. Por razones de economía procesal, es conveniente la tutela común de los parientes de las victimas, y no 200 procesos idénticos, en cuanto al objeto y demandado."*[188]

De tal manera, los derechos individuales homogéneos son derechos subjetivos individuales y divisibles, pero que por una situación de hecho o de derecho común se unen para resolverse en un solo proceso, en conjunto, sin perjuicio de que puedan ser

[187] SANCHEZ MORÓN, M citado por ROJAS RIVERO, Adriana. op.cit. P. 4.
[188] ROJAS RIVERO, Adriana. op. cit. P.5.

incoados de modo individual en la sede judicial correspondiente. Igual que en los intereses colectivos, en este tipo de derechos existe un vínculo jurídico o relación previa con los demandados.

Dentro de los derechos protegidos por los intereses supra individuales se encuentran los siguientes:

- Derecho a la paz.
- Derecho electoral.
- Derecho a un medio ambiente sano.
- Derecho a la seguridad ciudadana.
- Derecho a la salud.
- Derecho de los consumidores.
- Derecho a la no discriminación.
- Derecho de género.
- Derecho de los trabajadores.
- Derecho a la protección de bienes o valores culturales o históricos.

En lo que corresponde al tema objeto de investigación, los intereses supra individuales son materia del derecho de los consumidores pueden ser vistos en dos

jurisdicciones, a saber, la civil o el contencioso administrativo. La primera será la competente cuando de trate de violaciones realizadas por entes privados y la jurisdicción contenciosa administrativa lo será cuando el agravio provenga de un ente público.

El Nuevo Código Procesal Contencioso Administrativo (Ley 8508), que entró a regir en el 2008, dispuso las reglas para los procesos colectivos en esta materia. Se introdujo la capacidad procesal para realizar dichos procesos en el artículo 9 del Código, sin embargo, la redacción del artículo corresponde a los derechos colectivos, pues hace referencia a grupos determinados o determinables. En el artículo 10 se le da legitimación activa a quienes invoquen la defensa de los intereses colectivos y difusos, por lo que se reconoce el derecho de accionar por intereses colectivos y se brinda la legitimación de manera amplia.

En el artículo 48 de Código mencionado, se incluye la posibilidad de realizar un proceso unificado, cuando exista afectación de intereses y existan otros procesos con identidad de objeto y causa. Además, se establece en el artículo 185 la posibilidad de extender los efectos de lo dispuesto en al menos dos votos del Tribunal Contencioso o la Sala Primera que reconozcan una situación jurídica cuando exista identidad en objeto y causa con lo ya resuelto.

En la legislación española, los procesos colectivos son clasificados de acuerdo a los tipos de pretensiones o según el grupo de afectados[189]. En cuanto a las pretensiones, se dividen en acciones declarativas, de retractación, de cesación, de restitución o devolución, de reparación o indemnizatoria. En cuanto a los afectados, se dividen en: acciones de representación de intereses colectivos y acciones en representación de intereses difusos.

Una de las características de los procesos colectivos es que una vez que se da la sentencia, si ésta es favorable, beneficia a un colectivo de personas sin que sea necesario que se apersonen todas al proceso, es decir, sus efectos se extienden a una colectividad que no está siempre necesariamente determinada, por lo que no hace falta que acudan de manera individual a realizar un nuevo proceso con idéntica causa para obtener ese resultado beneficioso.

Cuando se habla de procesos colectivos es muy usual realizar una comparación o por lo menos visualizar a modo de referencia el denominado *class action* del derecho del *common law* norteamericano y aunque tienen elementos similares existen diferencias entre estos institutos. Por ejemplo, en el *class action* la legitimación activa la tiene

[189] MATEOS FERRES, María (2009). Procesos colectivos en materia de consumo de los servicios financieros. IX Jornadas de AUSBANC Internacional: Nuevos Derechos Financieros del Siglo XXI. San José, Costa Rica. 02 de Octubre de 2009. [Ponencias recopiladas en Disco Compacto]

cualquier interesado en el proceso, y no únicamente los indicados taxativamente, además pueden ejercerse en relación con cualquier tema.

Los derechos de los consumidores muestran características que los relacionan con los intereses difusos, por ejemplo, en cuanto al grupo que abarca y su determinación, pues en una situación específica puede verse afectada una gran cantidad de personas y muchas otras pueden tener posibilidades de afectación, piénsese v.g. en una situación de consumo de un alimento que contenga elementos tóxicos, el total de consumidores que se ven perjudicados o pueden verse perjudicados por el consumo de dicho producto no tiene límites nítidos de determinación, en efecto es el interés de todos el que se ve vulnerado.

Ahora bien, los derechos de los consumidores también abarcan características de los intereses colectivos, pues una vez organizados como grupo los consumidores afectados por alguna situación se vuelven un sector identificado y definido, y pueden acudir al reclamo de sus intereses de grupo.

Bajo estos supuestos se ubica el primer proceso colectivo en materia del consumidor que se lleva en Costa Rica, iniciado por la Asociación de Consumidores Libres (ACL) en representación de sus asociados víctimas de delitos informáticos y usuarios de la Banca

Estatal. Este proceso con arranca con 70 víctimas, de aproximadamente 900 víctimas que se vieron afectadas principalmente entre el 2007 y el 2008, en este momento se cuenta con aproximadamente 200 adheridas al proceso.

El proceso colectivo se hace ante el Juzgado de lo Contencioso Administrativo y Civil de Hacienda, en reclamo de los intereses colectivos y difusos de los consumidores de los servicios de Banca por Internet de las entidades bancarias estatales Banco Popular, Banco de Costa Rica y Banco Nacional. En esta demanda se solicita la indemnización por daño material y por daño moral.

Además, la ACL alega en su demanda que existen una serie de derechos vulnerados por las entidades bancarias, entre ellos el derecho a la información, derecho a la protección de datos personales, derecho a la seguridad, derecho a la protección de los intereses económicos, derecho a la publicidad no engañosa.

El daño material se pide argumentando que existe un nexo causal entre un hecho y un daño provocado por el actuar riesgoso de los bancos, pues se ofrece un servicio a través de la página WEB de los bancos para realizar transacciones electrónicas, actividad que implica un beneficio económico para los bancos, sin las medidas de seguridad idóneas para proteger los intereses económicos de los usuarios. Esta omisión de

seguridad permitió que a los clientes les fueran robados sus datos personales y se suplantara su identidad en los sitios virtuales bancarios, y de este modo se realizaran transacciones no autorizadas para sustraer su dinero, lo que implica sin duda alguna un daño en el patrimonio de los usuarios, daño que se consumó con ocasión al servicio brindado.

Las entidades bancarias son responsables, según la posición de la ACL, por ser parte de una cadena contractual, productor de un servicio, y como tal responde de los daños que de él se deriven. De este modo, se advierte que la responsabilidad en la que incurren los bancos es de tipo objetiva. Además, se considera que de acuerdo a los hechos, los bancos no se encuentran eximidos de responsabilidad objetiva, pues no se encuentran presentes las eximentes estipuladas por ley en este supuesto.

La ACL es clara en su posición de salvaguardar los intereses de los consumidores, ya que considera que no fueron provistos de información adecuada, completa y veraz sobre los riesgos que conllevan la actividad de Banca por Internet. Bajo esta perspectiva, no puede ser responsable un cliente que no conozca que debió tener determinado cuidado y no lo tuvo, pues en su actuar no hubo conocimiento ni voluntad, no sabía realmente los riesgos que podían generarse en este medio. Esta omisión de información responsabiliza a las entidades bancarias por los daños sufridos por sus clientes, en el entendido que son

los primeros quienes tienen una posición de superioridad frente al usuario y son los que poseen la información y el conocimiento técnico sobre la actividad.

Dentro de la demanda también se toca el tema de los contratos bancarios y las cláusulas abusivas. Los contratos para utilizar los servicios de Banca *Online* son contratos de adhesión, es decir, las cláusulas son estipuladas por una de las partes y la otra las acepta sin posibilidad de negociar. Para la ACL, algunas de las cláusulas dispuestas en estos contratos con cláusulas abusivas y se encuentran viciadas pues delegan toda la responsabilidad al cliente en caso de que sufra un daño, por ejemplo, denuncian el artículo 4 del Reglamento de Banca Electrónica del Banco de Costa Rica, que indica lo siguiente en su párrafo primero:

> ***"Artículo 4.*** Para el ingreso a los diferentes servicios que ofrece la Banca Electrónica, el Banco suministrará al cliente una clave de identificación o PIN, individual y secreto**, asumiendo el usuario toda la responsabilidad si por descuido, por su decisión o por acciones de terceros, la clave o PIN fuere de conocimiento de otras personas.** (…)" (El resaltado no es del original)[190]

[190] Reglamento de Servicios de Banca Electrónica del Banco de Costa Rica (2004), acuerdo Junta Directiva en sesión 10-04, publicado en el diario oficial La Gaceta 81 del 16 de marzo del 2004. Costa Rica.

Del mismo modo, se acusa el artículo 7 de citado Reglamento, que establece:

> *"**Artículo 7.** El usuario se obliga a conocer y aplicar en forma correcta las instrucciones de operación de los sistemas ofrecidos por el Banco. **El Banco queda relevado de toda responsabilidad por los daños que al usuario le puedan resultar a causa del desconocimiento o mal uso de dichos sistemas**."*[191] (El resaltado no es del original)

Estos artículos son sólo dos ejemplos de varios otros que fueron denunciados como abusivos, no solamente de esta entidad bancaria, sino también del Banco Nacional y del Banco Popular que figuran como demandados. Es común encontrar este tipo de cláusulas en los contratos y reglamentos de las entidades bancarias tanto estatales como privadas, y para la ACL se encuentran viciadas de nulidad, pues infringen los derechos de los consumidores fijados por la Constitución Política y leyes especiales.

Con este tipo de cláusulas, los bancos pretenden librarse de responsabilidad, lo que para la ACL constituye un abuso de derecho y por eso, se violentan los derechos de los consumidores, en el tanto no se respeta la buena fe y se fomenta un desequilibrio en la relación.

[191] Ibídem.

La ACL es enfática en su demanda en que este tipo de disposiciones que pretenden librar de responsabilidad a los bancos y generan una presunción de culpabilidad de los consumidores son abusos del derecho. El hecho que en operaciones fraudulentas se utilice el PIN del usuario por un tercero no significa de modo automático que existió una negligencia por parte del cliente.

Las pretensiones del proceso colectivo se dividen en cuanto a intereses difusos e intereses colectivos; en relación con los primeros, se solicita que los bancos adopten medidas para la protección de los intereses económicos de sus clientes, la protección de datos personales, mejorar la seguridad por Internet, brindar información veraz y clara que advierta sobre los riesgos y peligros de sus servicios, en estricto cumplimiento del derecho a la información, que se cree un seguro colectivo por fraude informático y se obligue a los bancos a obtenerlo.

En el tema del seguro, la ACL se presenta optimista en cuanto a esta posibilidad, pues se considera que se le daría una solución rápida y eficaz al cliente, lo que solucionaría por lo menos desde la óptima netamente del consumidor, el problema al que se ve sometido cuando es víctima de un delito informático y debe tal y como está la situación actual, afrontarse a toda una serie de procesos largos y a la expectativa de ver o no cumplidas sus pretensiones.

En entrevistas realizadas a representantes de los bancos, se preguntó sobre la posibilidad de adoptar este tipo de seguros, y se obtuvo una respuesta positiva, sin embargo, aún hoy este tipo de seguros no existe en el mercado, de acuerdo a la consulta realizada al Instituto Nacional de Seguros el 22 de febrero del 2010.

Continuando con las pretensiones, se solicita que se entregue a los clientes una copia del contrato de adhesión para banca por Internet, ya que algunos bancos no lo hacen; también se solicita la nulidad de las cláusulas abusivas de los contratos bancarios.

En cuanto a los intereses colectivos, se solicita que en los casos pendientes se dé por agotada la vía administrativa de las personas afiliadas a la ACL de conformidad con el artículo 31 inciso 4 del Código Procesal Contencioso Administrativo. También, que se declare la nulidad de la presunción de culpabilidad de los usuarios por el uso del PIN o clave secreta en operaciones fraudulentas por vulnerar el derecho de los consumidores, la condenatoria en abstracto de los daños materiales y morales, así como los perjuicios a favor de cada usuario afectado por la sustracción ilegítima del dinero de sus cuentas por medio de Internet afiliado a la ACL y por último, se solicita el pago de ambas costas a favor de la ACL.

En este proceso se realizaron en el 2009 dos audiencias preliminares, los bancos opusieron excepciones previas, sin embargo fueron denegadas. El Banco Nacional y el Banco de Costa Rica apelaron esta resolución, la apelación del Banco de Costa Rica fue declarada sin lugar, pero la del Banco Nacional no ha sido resuelta, por ello el proceso se encuentra en espera de resolución. Una vez que ésta se dé, se continúa con la Audiencia Preliminar pues aún hace falta la admisión de la prueba.

2.2 POSICIÓN DE LOS BANCOS

Los Bancos Estatales [192] han enfrentado múltiples demandas por Responsabilidad Bancaria frente al cliente por delitos informáticos, que han sido tramitados según lo indica la competencia, por el Tribunal Contencioso Administrativo o por la Sala Primera cuando se trata de casaciones. Durante los procesos enfrentados, a través de entrevistas y otros medios, los Bancos han manifestado su posición con respecto a esta situación.

[192] Se aclara, como se hizo *supra*, que la Banca Estatal es la que ha recibido demandas por delitos informáticos por su política de no conciliar, política que por ejemplo el Banco de Costa Rica ha decidido modificar actualmente. La Banca Privada también tuvo casos de clientes afectados por fraudes informáticos, sin embargo siempre decidió conciliar.

Esta opinión ha sido, a grandes rasgos, la de oponerse a la implementación de la Ley de Protección al Consumidor y su artículo 35 como solución para los casos de fraudes informáticos, argumentando que no existe responsabilidad que sea atribuida al banco por acciones que no han sido propias y se escapan de su esfera de control.

Los puntos clave del discurso bancario han sido los siguientes:

a. La relación que existe entre el Banco y el cliente contractual, pues el cliente firma un contrato en el que adquiere obligaciones y derechos; dentro de las obligaciones que adquiere está la de mantener un uso adecuado de sus contraseñas y claves de acceso, pues éstas son de uso personal y confidencial, es su deber mantenerlas en secreto y no revelarlas a terceras personas. Por lo tanto, existe una mala interpretación al querer adecuar la responsabilidad de los bancos a la establecida en la Ley 7472, pues el tipo de responsabilidad que existe es de orden contractual. El contrato es ley entre las partes, según el artículo 1021 del Código Civil.
b. La Ley Orgánica del Sistema Bancario Nacional en su artículo 60 le permite a los bancos establecer los términos y las condiciones de sus contratos.

c. Los clientes tienen la obligación de dar aviso al banco si se la ha extraviado o le han robado su cuaderno de cheques, de no hacerlo el banco se exime de responsabilidad. Esto ha sido así reflejado incluso en la jurisprudencia nacional, por lo que debe aplicarse el mismo principio a los casos del tema en cuestión.

d. Como se mencionó, una de las principales obligaciones de los clientes es la de no revelar sus claves de acceso o contraseñas de acceso a nadie, es su deber usarlas de modo personal y reportar al emisor el robo o pérdida de la tarjeta.

e. Internet no viene a revolucionar los contratos ni en su formación ni en sus efectos. La doctrina ha estimado que por la propia naturaleza del comercio electrónico, el consentimiento se otorgará sin que sea necesaria la presencia de las partes, originando con ello la necesidad de aplicar medidas de identificación extras para asegurar la identidad de los contratantes.

f. La contraseña del usuario equivale a su firma autógrafa, por lo tanto si se comprueba el adecuado acceso a la cuenta del cliente vía Banca por Internet con la contraseña de éste, se entiende que el cliente es quien ha ingresado al servicio.

g. El acceso a las cuentas del cliente por medio de la red Internet sólo puede ser realizado por quien tiene la clave y la contraseña que le fue habilitada al cuenta habiente.

h. El banco y el cliente son usuarios de la plataforma de comunicación denominada Internet, la cual es de acceso público. Los bancos no ofrecen al cliente el servicio de Internet, lo hace el respectivo proveedor del servicio de comunicaciones. La entidad bancaria le da al usuario la opción de accesar a sus cuentas, utilizando para este fin, dicha plataforma de uso público, esto significa que los medios utilizados para el fraude informático afectan al usuario de Internet por el hecho de ser él, aún y cuando no esté haciendo uso de los servicios del Banco en línea.

i. Si el cliente cae en engaño y entrega sus datos vitales sin su consentimiento sucede no porque el cuenta habiente sea usuario de los servicios del banco en forma electrónica, sino por el sólo hecho de ser usuario de la Internet, situación totalmente ajena al conocimiento y voluntad de los bancos.

j. Los usuarios de Internet, no sólo los clientes de la Banca por Internet, están expuestos a ser infiltrados por cualquiera de los programas que le pueden extraer sus datos sensibles. Es importante entender que el sistema de seguridad de los bancos está dirigido a impedir que sin la

clave de identificación correspondiente, haya una infiltración de un tercero no autorizado a las cuentas de sus clientes.

k. Los bancos no pueden impedir que el usuario asuma conductas que lo pongan en posición de riesgo de perder o fugar sus datos, aún cuando el cliente ni siquiera sea consciente de ello, pues ya es algo que puede ocurrirle al cliente por el sólo hecho de ser usuario del servicio de Internet.

l. Resulta inaplicable el régimen de responsabilidad extracontractual cuando es un hecho no controvertido que entre el banco y el cliente existe una relación contractual, pues existe un contrato de servicios bancarios, el tema en discusión tiene regulación diversa pues se fundamenta en la existencia de una contratación bancaria mercantil.

m. Bajo este presupuesto, los casos en cuestión deben resolverse de acuerdo a lo establecido por el Código Civil y el Código de Comercio.

n. Aún así, el artículo 35 de la Ley 7472 establece además de la responsabilidad objetiva, un criterio de ajeneidad, que permite eximir de responsabilidad cuando se comprueba que se ha sido ajeno al daño pues éste no se ocasionó por una acción u omisión del demandado, sino por razones ajenas a él.

o. El riesgo que el banco elimina es la posibilidad de que terceras personas puedan accesar al sistema de Banca por Internet, y no se ha logrado demostrar que se hayan vulnerado los sistemas de los bancos.

p. No es posible el acceso a las cuentas de los clientes sin claves o contraseñas. Ello por cuanto en el servicio de Banca por Internet existen controles de entrada que ineludiblemente le trasladan la responsabilidad al usuario, en cuanto a su guardia o custodia. Para el banco, si los accesos a la cuenta bancaria del cliente se hacen con la contraseña de éste entonces son accesos lícitos, normales y ordinarios.

q. Cuando se comprueba que el daño fue producto por hecho de un tercero ajeno al banco no puede imputársele la responsabilidad al banco. Con este hecho probado debe bastar para eximir de responsabilidad al banco y no además exigirle que compruebe que el cliente fue negligente o imprudente con el uso de sus contraseñas.

r. No se puede presumir la culpabilidad del banco porque el cliente aceptó contratar el servicio de Banca por Internet de modo libre y voluntario, el banco no le impuso el servicio. Además, el banco informó al consumidor y advirtió de eventuales fraudes informáticos.

s. Pretender hacer responsables a los bancos por fraudes informáticos, por las conductas activas u omisivas de los clientes es inaceptable y conlleva

una mala aplicación del artículo 35 de la ley mencionada, pues el riesgo de que al cliente se le haya infiltrado un tercero no es atribuible a los bancos.

t. La falta de cumplimiento de las obligaciones del cliente exime de responsabilidad al banco, cuando esa conducta de una u otra forma contribuye a producir la pérdida económica experimentada.
u. La cláusula del contrato de Internet que obliga al cliente a resguardar la clave no es abusiva y de hecho tiene su homólogo en la normativa de tarjeta de crédito.
v. El servicio ofrecido es 100% seguro y los riesgos deben asumirlos los usuarios cuando realizan un mal manejo de sus datos confidenciales.

Las entidades bancarias que han sido demandadas, han sostenido este tipo de argumentos pues desde su punto de vista la responsabilidad por delitos informáticos contra sus clientes no les es achacable. Han indicado también que a pesar de que no existe ningún estándar establecido que los obligue a tomar determinadas medidas para proteger sus sistemas y mantener una adecuada seguridad, ellos se han dado a la tarea de investigar y utilizar la última tecnología en sus sistemas para proporcionar la máxima protección al cliente y al banco.

Los bancos manifiestan que han invertido e invierten mucho dinero en la seguridad de las operaciones y en mecanismos adecuados para su protección. Muestra de ello es que para disminuir los porcentajes de fraudes informáticos, los bancos han empleado distintos elementos que sirven como mecanismos de doble autenticación, por ejemplo, los tokens y claves aleatorias. Estas medidas se han tomado con el objetivo de dotar al cliente de un instrumento que proporcione mayor seguridad y además para cumplir de una mejor manera con los principios de integridad, autenticidad, no repudio y confidencialidad. Sin embargo, aunque no puede negarse que se han logrado disminuir la cantidad de víctimas por delitos informáticos, esta cifra nunca ha dejado de tener un número considerable, lo que indica que la medida en sí no ha sido efectiva en un cien por ciento.

Recientemente, algunos bancos, entre ellos el Banco Nacional y el Banco Popular, han incluido la firma digital como una alternativa de seguridad. Este dispositivo, según como se estudió en el capítulo dos, proporciona de manera más completa la seguridad a las operaciones electrónicas, pues brinda un alto porcentaje de certeza en cuanto a la autenticidad, integridad y confidencialidad de los mensajes enviados entre las partes. Este sistema debe ser proporcionado junto con una capacitación adecuada que le permita al usuario el completo entendimiento del funcionamiento del sistema, sus alternativas y riesgos, para que pueda utilizarlo y

aprovecharlo de manera óptima, ya que no basta con dotarlo de una herramienta de última tecnología si no sabe cómo utilizarla.

Volviendo al tema de los argumentos esbozados por los bancos, ha sido incluido como punto de inconformidad en sus recursos de Casación, en el caso específico por el Banco Nacional, que el servicio de *Internet Banking* no ofrece el cien por ciento de seguridad. Es de su criterio, que el servicio del banco no falló, pues se trata de una ventanilla de acceso a la cuenta del cliente y en esos términos a funcionado de manera eficiente sin que en ningún momento se hayan vulnerado los sistemas del banco.

Se arguye también por esta entidad bancaria que, en el contrato de *Internet Banking* se advierte sobre los cuidados y riesgos del servicio, además que siempre se ha mantenido información pública sobre el tema, así como reportajes en la prensa. Consideran que los riesgos de la red son harto conocidos *erga omnes*, públicos y notorios.

En cuanto a los reclamos esbozados por el Banco de Costa Rica en sus recursos de Casación, se encuentra que se ha dado una mala interpretación del artículo 35 de la Ley de Protección al Consumidor, pues se entiende que la responsabilidad objetiva por el servicio de Banca por Internet se extiende a todos los focos de riesgo que le resultan

ajenos, con lo que se produce una socialización de cualquier riesgo que surja de las relaciones de consumo que se verifiquen al amparo del canal de acceso, a pesar de que en la administración del servicio brindado por el Banco, se cuenta con los más altos estándares de seguridad, pero en el canal de acceso el Banco no ejerce control alguno, resultando absolutamente ajeno a éste. Los riesgos típicos, propios e independientes al sistema de banca electrónica deben ser asumidos por sus prestatarios, no por la entidad financiera. Manifiesta que el servicio ofrecido por el intermediario y respecto del cual el banco obtiene un beneficio es absolutamente seguro, no así el manejo del nombre del usuario y la clave de seguridad o PIN. El sistema del Banco es, según su interpretación, invulnerable al ataque de terceros que pretendan obtener los datos personales de los clientes, a fin de acceder a las cuentas respectivas.

A partir de las sentencias tanto del Tribunal Contencioso Administrativo como de la Sala Primera, que serán analizadas en la siguiente sección, los Bancos han tomado diversas actitudes. De todos los casos que han sido resueltos, solamente en uno de ellos se logró determinar que existió culpa de la víctima y por lo tanto operó este eximente de responsabilidad, la sentencia fue a favor del Banco Nacional. En todas las demás resoluciones ha sido constante el criterio de Responsabilidad Objetiva de las entidades bancarias. Es por ello que el Banco de Costa Rica ha decidido negociar vía conciliación con las víctimas de fraudes informáticos y lograr una solución alternativa

sin necesidad de acudir a los Tribunales de Justicia. Por su parte, el Banco Nacional, amparado en el voto favorable que obtuvo en la Sala Primera, ha decidido continuar con su política de no conciliación y que se resuelva el conflicto tal y como se ha venido haciendo, en sede judicial.

Por su parte, el Banco Popular ha tenido resultados muy positivos con la aplicación del Sistema de Favoritos como mecanismo de seguridad, ya que ha logrado disminuir prácticamente en su totalidad los casos de fraudes informáticos contra sus clientes. Aunado a lo anterior, como se mencionó *supra*, ofrece en la actualidad el sistema de firma digital.

SECCIÓN III

ANÁLISIS DE LAS SENTENCIAS SOBRE RESPONSABILIDAD OBJETIVA EN EL SERVICIO DE BANCA POR INTERNET: TRIBUNAL CONTENCIOSO ADMINISTRATIVO Y SALA PRIMERA

3.1 RESOLUCIONES DEL TRIBUNAL CONTENCIOSO ADMINISTRATIVO

El tema de la Responsabilidad Bancaria frente al cliente por delitos informáticos ha sido novedoso en nuestra jurisprudencia, pues hace muy poco tiempo no existía nada en concreto que indicara un punto referencial al respecto. Cuando los usuarios bancarios se enfrentaron a este tipo de problema, no tenían ninguna idea concreta de cómo iba a resolverse su situación. En la misma situación se encontraban los bancos, quienes no sabían qué indicaciones debían seguir para dar resolución a este tipo de conflictos. En este cuadro fáctico se someten los casos a la decisión de los jueces de la República, para que sean éstos quienes diriman el conflicto. En esta instancia, se encuentra la misma incertidumbre de las partes sobre este tan desconocido tema en

ese momento, cómo resolver, qué tesis acoger, a quién se debe proteger. Bajo estas interrogantes, el Tribunal Contencioso Administrativo emite sus primeros criterios.

El Tribunal Contencioso Administrativo ha sido consecuente desde su primera resolución hasta las más recientes: los bancos, acogiendo la tesis de los actores (clientes bancarios), son responsables objetivamente por los daños sufridos por los consumidores de servicios bancarios por Internet, en razón de obtener un beneficio patrimonial de una actividad y consecuentemente crear un riesgo para sus clientes, encajando los elementos de esta actividad dentro de lo estipulado por el Derecho del Consumidor en su Ley especial 7472.

En el análisis del Tribunal mencionado, se determina que entre los Bancos que prestan el servicio de Banca por Internet y los clientes, usuarios de este servicio, existe una típica relación de consumo, siendo que el Banco funciona como el proveedor tal y como lo define la Ley de Protección al Consumidor, y el cliente tiene el papel del consumidor. En este tanto, el régimen determinado por la Constitución Política y la ley para las relaciones de consumo es el estipulado en la Ley antes citada.

Esta Ley incorpora en su artículo 35 el régimen de Responsabilidad Objetiva:

"ARTÍCULO 35.- Régimen de responsabilidad.

El productor, el proveedor y el comerciante deben responder concurrente e independientemente de la existencia de culpa, si el consumidor resulta perjudicado por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su utilización y riesgos.

Sólo se libera quien demuestre que ha sido ajeno al daño.

Los representantes legales de los establecimientos mercantiles o, en su caso, los encargados del negocio son responsables por los actos o los hechos propios o por los de sus dependientes o auxiliares. Los técnicos, los encargados de la elaboración y el control responden solidariamente, cuando así corresponda, por las violaciones a esta Ley en perjuicio del consumidor.

(Así modificada su numeración por el artículo 80 de la ley N° 8343 de 27 de diciembre del 2002, Ley de Contingencia Fiscal, que lo pasó del 32 al 35)"[193]

[193] Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, N° 7472 de 20 de diciembre de 1994. Artículo 35.

Una vez definido el ámbito jurídico en el que se desenvuelven las partes, se establecen de modo recíproco una serie de obligaciones y derechos que deben ser cumplidos. Dentro de las obligaciones de los Bancos se encuentran el suministrar el servicio de forma segura, ininterrumpida y de forma informada. Por ello, debe proporcionarle al consumidor información suficiente para que éste realice una decisión con el panorama completo de riesgos y beneficios.

En el caso en particular de la Banca por Internet, el cliente necesariamente debe accesar a la red pública Internet para poder ingresar a la página bancaria. El banco entonces se vuelve un proveedor de servicios en Internet. Se aclara que el banco no provee el servicio de Internet, pero siempre mantiene una relación o vinculación contractual con ellos pues necesita de ellos para poder mantener el servicio de Banca *Online.*

La responsabilidad para el Banco surge en el momento en que un cliente se ve perjudicado o dañado en razón al servicio que se le ofrece, y se demuestra que éste generó un riesgo. Nace ahí la responsabilidad contractual objetiva. Para responsabilizar al ente bancario debe probarse el nexo causal, es decir, verificar que el hecho o la omisión del banco es la causa directa, eficiente e inmediata del daño provocado. El riesgo se genera en el servicio prestado, si el banco presta un servicio de intermediación financiera

y de custodia de valores, entre otros, y obtiene por ello un lucro, debe tener altos estándares de seguridad. Pero además, si decide adoptar el uso de nuevas tecnologías, como lo son los medios virtuales para brindar su servicio, debe asumir la responsabilidad que se pueda derivar de ello, pues está creando un riesgo al ofrecer el servicio, riesgo que es inherente a la actividad y donde está indisolublemente ligada la seguridad, riesgo que ha sido incluso admitido por los mismos bancos. Es criterio del Tribunal Contencioso Administrativo que si quiere dar el Banco un servicio de avanzada, debe también proveer a sus clientes de la seguridad adecuada.

El riesgo consiste en que las medidas de seguridad para proteger al cliente eran consideradas primarias, pues sólo se contaba con mecanismo de autenticación, la contraseña o PIN, lo que definitivamente no era suficiente para otorgar seguridad al usuario.

Sólo se libera el que demuestre que es ajeno al daño, según el mismo artículo 35 citado lo indica, y esto es si se demuestra que existió culpa de la víctima, fuerza mayor o hecho de un tercero. Estas eximentes no fueron demostradas por el banco, según el Tribunal Contencioso Administrativo, por lo que no hay manera de desligar su responsabilidad.

El Tribunal Contencioso Administrativo, en su mayoría, admite que el banco no proporcionó al cliente la información adecuada y necesaria para que estuviera consciente de los riesgos del servicio puesto a su disposición, además que no le permitió negociar las cláusulas contractuales que iban a regir su relación, ya que el contrato es de adhesión y sin posibilidad de no estar de acuerdo en alguna de sus disposiciones. Se dispuso también que a pesar de que la Ley 7472 establece eximentes de responsabilidad, si se demuestra una de ellas, pero el banco produjo un riesgo y el daño se materializó a través de este medio riesgoso, el banco no se exonera de responsabilidad.

Merece particular atención la sentencia número 743-2008 de las catorce horas diez minutos del veintiséis de setiembre del dos mil ocho, por cuanto la decisión de responsabilizar al Banco se tomó por mayoría, siendo que el juez Alner Palacios salvó su voto, al considerar fundamentalmente que quedó demostrado que para accesar a la cuenta bancaria vía Internet Banking, es obligatorio el ingreso de una contraseña o PIN que corresponda con el usuario. Por ello, el juez Palacios considera que la vulnerabilidad radicaría en que un tercero pueda ingresar a la cuenta bancaria de un cliente sin necesidad de agregar estos datos, bajo este presupuesto el sistema del Banco no sería seguro y sí correspondería la responsabilidad objetiva. Si un tercero logra obtener las contraseñas y claves, habría que analizar de dónde las obtuvo, por ejemplo, si se debió a un mal manejo del banco o cuando un tercero utiliza medios informáticos para obtener

los datos confidenciales, caso en el que la vulnerabilidad se presentaría pero desde el cliente.

Para este juez, el cliente se ve afectado no en razón de la actividad del banco, sino por el canal que necesariamente debe utilizar para accesar a sus cuentas vía Internet, es decir, se ve afectado por el hecho de ser cliente de Internet, no del banco. El banco, según su criterio, ha informado debidamente al cliente sobre los riesgos y usos adecuados de sus datos personales, y no puede hacerse responsable de las conductas inadecuadas de éste. El régimen jurídico que rige en este tipo de situaciones, por existir un contrato de por medio, es el mercantil.

Acogiendo la Teoría del Riesgo, para el juez Palacios opera la eximente de responsabilidad de hecho de un tercero, en contraposición a la opinión de sus compañeros del Tribunal. Para el esto fue demostrado en el tanto se probó que no existió participación del Banco en el hecho delictivo, y obligarlo a probar además que el usuario fue negligente en el uso de sus claves y contraseñas sería desproporcionado.

Este criterio se apega a los argumentos bancarios, sin embargo, no es el que sostiene la mayoría del Tribunal Contencioso Administrativo. Más bien, se han sentado múltiples precedentes que han provocado un cambio en la actitud de algunos de los

bancos, por ejemplo, el Banco de Costa Rica, quien ha decidido implementar la conciliación a raíz de las condenas que ha recibido en esta sede y en la Sala Primera.

3.2 RESOLUCIONES DE LA SALA PRIMERA

A raíz de las sentencias del Tribunal Contencioso Administrativo, se han elaborado recursos de Casación con el fin de modificar lo resuelto por este Tribunal. La Sala Primera es la encargada de dar la sentencia definitiva, de establecer el criterio final para la resolución de estos conflictos.

En concordancia con lo estimado por el Tribunal Contencioso Administrativo, la Sala Primera ha confirmado el criterio de responsabilizar a los Bancos con base en la Teoría del Riesgo creado incluida en la Ley de Protección al Consumidor. Esta decisión ha sido tomada con fundamento en una serie de argumentos que a continuación se resumen.

En Costa Rica se ha adoptado la Teoría de la Causalidad Adecuada, que fue explicada en el Capítulo Primero, consistente en que debe existir una vinculación entre daño y conducta cuando el primero se origine, si no necesariamente, al menos con una alta probabilidad según las circunstancias específicas que incidan en la materia de la segunda.

Los eximentes de responsabilidad: fuerza mayor, culpa de la víctima, hecho de un tercero, actúan sobre el nexo de causalidad, descartando que la conducta atribuida a la parte demandada fuera la productora de la lesión sufrida. Se tienen como parte de una relación de consumo a la existente entre los bancos y sus usuarios, pues el primero encaja dentro del concepto de productor, proveedor o comerciante de un servicio y el cliente como consumidor que tiene la posibilidad de adquisición, disfrute o utilización de un bien.

> *"El Banco actúa en ejercicio de su capacidad de derecho privado, como una verdadera empresa pública, y en su condición, ofrece a sus clientes un servicio, por lo que, al existir una relación de consumo, el caso particular debe ser analizado bajo el ámbito de cobertura del numeral 35 en comentario."*[194]

El riesgo que es eficiente para crear responsabilidad debe ser anormal, que se exceda del margen de tolerancia que resulta admisible de acuerdo a las reglas de la experiencia, lo que debe ser evaluado en forma casuística por el juez. La persona a la que se le imputa el daño debe ser la que se encuentre en una posición de dominio con respecto a aquel, quien desarrolla la actividad o asume las posibles consecuencias

[194] Sala Primera de la Corte Suprema de Justicia. Sentencia 00300-F-S1-2009 de las once horas con veinticinco minutos del veintiséis de marzo del dos mil nueve.

negativas asociadas, recibiendo un beneficio de ello. La víctima debe probar el daño sufrido y el nexo de causalidad, mientras que el demandado debe probar alguna de las eximentes de responsabilidad objetiva o que este régimen no le es aplicable.

Para la Sala Primera, en materia de seguridad los esfuerzos deben ser continuos y acordes a los más altos estándares de seguridad. En los casos puestos en su conocimiento quedó demostrado que la plataforma informática de los bancos no fue vulnerada para obtener la clave y el usuario de los clientes. La seguridad con que cuentan las entidades financieras resulta adecuada para proteger la integridad de la base de datos y la plataforma transaccional a lo interno.

> *"Se debe, sin embargo, tomar en cuenta que la entidad financiera tiene como función esencial la intermediación financiera, que incluye la captación de fondos provenientes del ahorro público, concepto que lleva implícita su custodia, tanto desde el punto de vista físico, como del registro electrónico correspondiente. Tiene una ineludible obligación de garantizar la seguridad de las transacciones realizadas, ya sea desde ventanilla o mediante cualquier otro puesto a disposición de los clientes."*[195]

[195] Ibídem.

En su criterio, la Sala confirma que la responsabilidad que le fue imputada al banco se fundamenta no en la sustracción del dinero, sino en la existencia de un riesgo en el funcionamiento del propio servicio que se ofrece, lo que permite imputar el origen del daño al funcionamiento del servicio. Lo anterior a pesar de disponer de mecanismos que permiten mayor seguridad.

En la mayoría de las sentencias existentes hasta ahora, a excepción de una resolución que será analizada más adelante, la Sala Primera ha considerado que no se ha logrado desvirtuar el testimonio de los afectados para comprobar una culpa de la víctima como eximente de responsabilidad. Esto porque no ha logrado desvirtuarse la versión de las víctimas con respecto al resguardo de sus contraseñas o claves de acceso, sin las cuales no es posible ingresar a sus cuentas bancarias. Es también justamente en este punto donde surge el riesgo que crea el banco, al no tener un adecuado sistema de autenticación que permita comprobar de manera más segura la identidad del cliente, riesgo del que pueden aprovecharse terceras personas conscientes de esta debilidad.

Se tiene por cierto que Internet no forma parte del servicio que ofrecen los bancos, sin embargo, se sirven de este medio para la prestación de un servicio, y este argumento de todos modos no funciona como eximente de responsabilidad. Se ha sostenido que por lo delicado de la actividad, los márgenes de exigibilidad en diligencia, seguridad,

eficiencia, cuidado y razonabilidad en el manejo aumentan. Los bancos responden no sólo por la fortaleza de sus sistemas internos, sino también por la seguridad de quien para llegar allí, utiliza los únicos canales posibles que el propio Banco conoce y reconoce como riesgosos. Y responden no en cuanto ajenos, sino en la medida que constituye un medio del que se prevalece, directamente, para la prestación del servicio.

> *"El medio para acceder a la plataforma del Banco no se trata, por ende, de un foco ajeno de riesgo, sino de un instrumento consustancial al servicio que presta, si se quiere, forma parte intrínseca de la actividad, que si bien es accesorio a la actividad del intermediario, resulta imprescindible. Los mecanismos de garantía al cliente –usuario- deben darse no sólo dentro de los muros informáticos del propio Banco, sino también en el camino de acceso a él como parte del servicio."*[196]

La Sala Primera, sin embargo, no concuerda con lo manifestado por el Tribunal Contencioso Administrativo en cuanto a que a pesar de demostrarse la existencia de una eximente de responsabilidad igual opera la Responsabilidad Objetiva pues existe un riesgo creado por los bancos. Para esta Cámara, si se toma el artículo 35 de la Ley de Protección al Consumidor como el parámetro general sin determinar casuísticamente la

[196] Ibídem.

existencia de un nexo causal, se haría inoperante el criterio de ajeneidad que está establecido justamente en el mencionado artículo, con lo que se incurre a la socialización absoluta de cualquier riesgo que surja en la totalidad de las relaciones de consumo.

En cuanto a lo alegado por los bancos en relación con a la existencia de una relación contractual que debe ser tomada en cuenta y no endilgar una responsabilidad extracontractual como se ha querido hacer utilizando la Responsabilidad Objetiva, además que en este contrato se advierte sobre los cuidados y riesgos, la Sala Primera determinó que no debe perderse de vista que el objeto del proceso es determinar si existe en cada caso responsabilidad al amparo del precepto 35 de la Ley 7472, es decir, el análisis en esa sede se centra en la existencia de un riesgo que permite realizar la imputación del daño al ente estatal, así como la inexistencia de causas eximentes de responsabilidad. Aún y cuando se compruebe lo planteado por los bancos, ello no permite por sí mismo desvirtuar, si es el caso en la especie determinada, el fallo del Tribunal.

Se aclara por la Sala Primera que el régimen establecido en el artículo 35 de la Ley 7472 aplica tanto para los supuestos de responsabilidad extracontractual como contractual, independientemente en esta última del incumplimiento de los acuerdos inter partes que regulan la relación específica. El surgimiento del deber de reparar surge

de la existencia de los supuestos exigidos por la disposición correspondiente, sean el daño, la conducta lesiva, el nexo causal que vincula los dos anteriores y el criterio de imputación determinado, en estos casos, la teoría del riesgo creado.

Finalmente, no aprecian los magistrados que las sentencias impugnadas hayan sido desproporcionadas o hayan dejado de aplicar en modo indebido los principios constitucionales, antes bien, se considera que se ha procurado la protección del consumidor frente a su contra parte comercial tal y como lo determinan los artículos 41 y 46 de la Constitución Política.

Como se adelantó, todas las sentencias a excepción de una, han ido enrumbadas en el mismo camino de atribuir la responsabilidad de los bancos, confirmando en lo consecuente el criterio de primera instancia. No obstante, en la sentencia de Sala Primera 000516-F-S1-2009 de las diez horas veinte minutos del veintisiete de mayo del dos mil nueve, en casación presentada por el Banco Nacional, se determinó la existencia en el caso concreto de una eximente de responsabilidad: la culpa de la víctima.

En este caso, según lo informó la propia víctima, recibió un correo electrónico sospechoso que empezó a completar, sin recordar qué partes completó, sin embargo, indica que no envió el correo. Con estos hechos, la Sala Primera dio por probado que no

existió un nexo causal entre el hecho alegado y el daño, pues la propia víctima reconoce haber suministrado una serie de datos, entre los que pueden encontrarse datos confidenciales, en un correo que cataloga como sospechoso. En este caso, para el juzgador existe un daño ocasionado por la imprudencia y mal manejo de sus contraseñas y claves personales de la propia víctima y no en el funcionamiento inadecuado del servicio que presta el intermediario bancario.

El usuario, aunque se encuentre dentro de una relación en la que aplique la Teoría del riesgo creado, no se exime de tener cierto grado de prudencia en el manejo de sus claves y datos personales, debe tener un nivel medio de diligencia en el manejo de los datos que le incumben. En este caso, según argumenta el órgano decisor, la víctima no tuvo ese deber de cuidado y ello contribuyó para que se le ocasionara un daño. Aunado a esto, la víctima no dio aviso al Banco ni tuvo ninguna conducta previsora que impidiera la concreción de un daño. Es por estas razones que por mayoría de decide declarar con lugar el recurso de casación y declarar sin lugar la demanda.

Al respecto, existe un voto salvado de los magistrados Román Solís Zelaya y Óscar González Camacho, quienes se apartan del criterio de la mayoría y sostienen el criterio mantenido para el resto de sentencias que ha resuelto este órgano superior. Se indica principalmente que existe duda en cuanto a la información que suministró la víctima y si

en efecto se envió o no el correo sospechoso, por lo que no puede presumirse que definitivamente fue por su actuar negligente que se obtuvieron sus contraseñas y claves. Para estos magistrados, no existen elementos probatorios que permitan concluir que existió incumplimiento del deber de cuidado y prudencia por parte de la actora.

SECCIÓN IV

POSICIÓN PERSONAL SOBRE EL TEMA

Una vez analizado el tema propuesto, iniciando por el estudio de la Responsabilidad Civil, su desarrollo doctrinario y jurisprudencial, los delitos informáticos y medidas de seguridad desarrolladas y adoptadas, arribando finalmente al análisis de la cuestión que se discute en este proyecto, con los elementos necesarios para emitir un criterio informado y objetivo, pero sobretodo con el fin de brindar una perspectiva que aporte una alternativa a un punto tan reciente y tan discutido en el Derecho Costarricense, se procede a emitir una opinión personal.

La responsabilidad bancaria por delitos informáticos sufridos por sus clientes existe y se determina con base en la Teoría del Riesgo Creado traducida en la Responsabilidad Objetiva, de la que ya se ha hablado con amplitud durante el presente trabajo. Es criterio personal que en correcta aplicación del derecho debe emplearse el régimen establecido en la Ley de Protección al Consumidor por tratarse indudablemente de una relación de consumo. El banco encaja dentro del concepto de proveedor que establece la ley mencionada y el usuario hace lo mismo dentro del concepto de

consumidor, siendo que el servicio que se presta, Banca por Internet, viene a ser el punto que une en la relación de consumo a las partes.

Es cierto que la relación se encuentra enmarcada en un Contrato firmado por las partes, sin embargo, la responsabilidad objetiva aplica también en el plano contractual, no únicamente en supuestos de responsabilidad extracontractual. Lo importante, como se ha dicho, es el riesgo creado y el daño producido como resultado o materialización de este riesgo, sin importar el tipo de relación preexistente a ese daño.

De este modo, se considera que el Banco se encuentra obligado a responder civilmente por los daños sufridos por el consumidor de Banca por Internet siempre y cuando se demuestre el nexo de causalidad. El Banco, tal y como se establece en casos de Responsabilidad sin culpa, debe probar en primer lugar si aplica para la situación determinada la utilización de la Responsabilidad Objetiva y en segundo lugar si operan las causas eximentes de responsabilidad. En el caso en que se compruebe que el caso no encaja en los presupuestos o que existan eximentes de responsabilidad, el Banco se exonera de responsabilidad por delitos informáticos contra sus clientes.

Así, debe definitivamente darse un análisis del juez caso por caso, para dar una solución correcta y justa. El análisis debe incluir un estudio en los elementos objetivos y

subjetivos del caso para determinar el tipo de responsabilidad por aplicar, el nexo de causalidad, con atención en la Teoría de la Ajeneidad y la Teoría de la Causalidad Adecuada.

El consumidor en Costa Rica ha sido dotado de una serie de derechos que son considerados fundamentales e irrenunciables, según la Constitución Política y los instrumentos creados para su Defensa, *v.g*. la Ley 7472. Dentro de los derechos que posee todo consumidor se encuentra el de ser informado adecuadamente sobre los servicios que se le ofrecen, incluyendo riesgos y demás consecuencias que puedan contener, para que el consumidor realice una decisión consciente e informada.

Es por ello que en todo servicio este requerimiento de información es obligatorio, sin que el servicio de Banca por Internet sea la excepción. Con base en la investigación realizada, así como en lo que ha sido determinado por los Tribunales de Justicia, los Bancos han fallado en cuanto a la información que debe dársele al cliente, y en criterio personal, se considera que no solamente se ha fallado en la información sino en la obligación de dar la capacitación adecuada al cliente que no es experto en temas de tecnología ni de informática, es decir, el ciudadano promedio.

No puede suponerse que la información va a ser adquirida por el cliente a través de canales distintos al proveedor del servicio, pues quien tiene el mayor conocimiento sobre el servicio que presta y especialmente, quien tiene el deber de educar al consumidor es el propio prestatario del bien o servicio.

La información debe ser completa en cuanto a los usos del producto, las medidas de seguridad que se deben tomar, de modo tal que sea entendible por el consumidor y éste asimile y demuestre su conocimiento para utilizar los servicios proporcionados. En este sentido, se propone que exista un mecanismo que permita capacitar al cliente de servicios bancarios vía Internet y al mismo tiempo que le compruebe a la entidad que en efecto los conceptos fueron debidamente comprendidos por los clientes.

La solución que se perfila es crear de modo obligatorio un programa que se ejecute la primera vez que se acceda a la página bancaria con el fin de ingresar a la cuenta bancaria y que sea un requisito indispensable para poder realizar cualquier operación, de modo tal que el programa incluya una capacitación desarrollada en lenguaje sencillo y comprensible, pero sobre todo claro y suficiente para que el cliente adquiera las herramientas necesarias que le permitan realizar un acceso seguro a su cuenta bancaria.

Además de la capacitación, el programa debe incluir una serie de exámenes o pruebas rápidas para comprobar el nivel de comprensión del conocimiento, hasta que el cliente apruebe el curso que le acredite como persona apta para utilizar la Banca *Online.* Esto se considera así, pues es una realidad que la red Internet y correlativamente los servicios que se brindan a través de ella son peligrosos y poseen un riesgo que no es eliminable al cien por ciento, entonces no parece ilógico tomar medidas para palear esos riesgos, dentro de los que definitivamente se ubican la capacitación y concientización, ya que no basta con tener tecnología de punta y sistemas con máxima seguridad para protegerse a lo interno y al usuario si el cliente, el sujeto para y por el que se desarrolla el servicio tiene una deficiencia.

Piénsese a modo ejemplo en la actividad de conducción, que es considerada una actividad peligrosa pero que es permitida bajo los límites propios del riesgo establecidos por el Estado. Para permitir que una persona conduzca, debe comprobarse que ésta tiene la capacidad teórica y práctica para hacerlo, y de este modo realizar la actividad bajo los parámetros del riesgo permitido. En cuestiones tecnológicas, en específico en cuanto a Internet *Banking,* el Banco como proveedor del servicio y potencial responsable de un daño sufrido en razón de esta actividad, debería adoptar una conducta tendiente a prevenir el daño y eliminar riesgos delimitando cuándo una persona ha adquirido los conocimientos suficientes para ser considerado apto para la utilización de Banca *Online*.

Se ha comprobado, que el desconocimiento y la falta o incorrecta información ha servido como portillo para que se generen los delitos informáticos.

Si los bancos se preocupan por educar al cliente, estarían tomando una medida más de seguridad, aún más efectiva que invertir en tecnología que el cliente no sepa usar y no sea por lo tanto efectiva. El planteamiento general en esta investigación es hacer una revisión de las medidas de seguridad adoptadas, tomando en cuenta lo que se considera un estadio más dentro de los mecanismos de seguridad exigibles, a saber, la concientización.

También, se piensa que es necesario el establecer un reglamento o instrumento que disponga las medidas mínimas con las que deben contar las entidades bancarias para brindar el servicio de Banca por Internet. Esto con el fin de que no existan desprotecciones al consumidor o inconsistencias en los niveles de seguridad ofrecidos, pues en este momento no existe ningún instrumento que regule de modo específico el sistema de seguridad considerado como adecuado para proveer el servicio de Banca Online.

Estas disposiciones pueden ser establecidas por el Banco Central o incluso la SUGEF o el CONASSIF, que cuentan con la competencia suficiente para reglar los temas

bancarios. Se pretende que este instrumento cuente con las medidas de seguridad consideradas como mínimas para prestar el servicio, sin que esto limite la posibilidad de que el Banco pueda brindar mecanismos con mayor seguridad de la establecida. Este instrumento debe ser sometido a una revisión periódica, dentro de los criterios racionales, ya que en temas de tecnología el cambio se produce a gran velocidad. Dentro de los instrumentos que pueden ser adoptados por los bancos en la actualidad se encuentra la firma digital y los certificados digitales, que como se ha mencionado, ya están siendo manejados por varias entidades, entre ellas el Banco Central.

En otro orden de ideas, se estima que es necesaria la revisión de los reglamentos internos de los Bancos así como de sus contratos con el fin de eliminar o modificar cláusulas abusivas. Por ejemplo, debe eliminarse la presunción de culpabilidad del cliente cuando un tercero obtiene de forma indebida sus contraseñas y claves. Si el Banco considera que la obtención de los datos confidenciales del cliente se dio por un mal uso, imprudencia, dolo, o en general por culpa de la víctima debe demostrar que así lo fue y no crear una causal de exoneración de responsabilidad que no está incluida dentro de los supuestos de la Ley 7472.

Se aplauden las políticas de algunos bancos, entre ellos el Banco de Costa Rica, de buscar un diálogo, el cambio en su trato al cliente y la búsqueda de una resolución

alterna de los conflictos con sus usuarios, pues se beneficia al consumidor pero también al Banco, en el tanto la cordialidad en las relaciones de las partes debe ser la regla y no la excepción, principalmente en una relación en la que las partes se necesitan una a otra, e incluso el Banco se debe al cliente para lograr subsistir. Por ello, el objetivo por cumplir debe ser, en la medida de lo posible, el sostener una relación pacífica y sana, sin pensarse en rivalidades ni antagonismos.

CONCLUSIONES

Una vez finalizada la investigación, se tienen como conclusiones las siguientes:

El tema de la responsabilidad bancaria frente al cliente por delitos informáticos es realmente novedoso en la doctrina y la jurisprudencia nacional, es por ello que ha sido necesario el análisis conjunto de diversas ramas del Derecho que funcionan de modo conjunto en todo lo que envuelve este conflicto.

La responsabilidad objetiva, como criterio de impugnación, ha ido desarrollándose cada vez más dentro de las legislaciones, con el fin de reparar los daños sufridos por las víctimas que se quedaban fuera del ámbito de protección del sistema de responsabilidad subjetiva. Así, se busca extender la protección que la ley puede dar a todas aquellas situaciones que generen un daño y que requieren ser indemnizadas.

En Costa Rica la jurisprudencia sobre Responsabilidad Objetiva es abundante y se ha incrementado a raíz de la Ley de Protección al Consumidor, que incluye en su artículo 35 el régimen de responsabilidad que rige para las relaciones de consumo, basándose en la Teoría del Riesgo Creado. De este modo, cubre de manera amplia todos aquellos

supuestos en los que encajen los presupuestos subjetivos y objetivos dentro de los conceptos de consumidor, productor, comerciante o proveedor y bien o servicio ofrecido. No se dejan de lado, los casos que están relacionados con los párrafos cuarto y quinto del artículo 1048, para los que también se ha determinado la aplicación de la Responsabilidad Objetiva.

En la época actual, la tecnología y la ciencia avanzan a pasos agigantados y con una enorme velocidad, dentro de las alternativas que la tecnología pone al alcance del ser humano se encuentra el Comercio Electrónico, y como un elemento de éste se ha desarrollado la Banca por Internet. Con ella se le brinda al cliente bancario accesar a sus cuentas vía Internet y realizar una amplia gama de transacciones desde su computadora. Este sistema crea una atractiva opción, que funciona con las necesidades del usuario actual, quien necesita celeridad en sus operaciones y facilidad en su ejecución, opción que con ajetreado día a día en la era moderna, les resulta ideal a los consumidores. Aunado a lo anterior, el movilizar cantidades considerables de dinero no resulta seguro hoy, lo que le otorga un valor agregado a la Banca *Online.*

Para adquirir los servicios de *Internet Banking* de la entidad bancaria de preferencia se firma un contrato que ha sido elaborado por el Banco y se comprometen las partes al cumplimiento de las cláusulas ahí establecidas. El contrato firmado es un

contrato de adhesión, en el que el cliente se limita a firmar y aceptar las disposiciones ahí manifestadas, sin posibilidad de negociación. Este tipo de negociación, sin embargo, no viene a revolucionar el modo de contratación ya establecido en las leyes civiles y mercantiles, pues mantiene los mismos principios para su elaboración, validez y eficacia, la única diferencia es el medio utilizado para realizarse.

A la par de las ventajas que proporciona la Banca por Internet se encuentran las herramientas que se han desarrollado con el fin tomar partido, de forma ilícita, de este moderno instrumento. Se desarrollan así una serie de delitos informáticos a través de los cuales los delincuentes cibernéticos pretenden obtener un beneficio patrimonial ilegítimo, defraudando al consumidor de servicios bancarios por Internet. Los más comunes, por su nivel de afectación al cliente, han sido el *Phishing*, el *Pharming*, el *Malware,* los *Key loggers* y los Troyanos o Caballos de Troya, entre otros.

Este tipo de delitos buscan obtener los datos confidenciales de los clientes, ya sea a través del engaño o de la instalación de programas ocultos dentro de la computadora, para utilizarlos en transacciones bancarias no autorizadas vía Internet y defraudar al cuenta habiente. En Costa Rica una gran cantidad de personas han sido víctimas de este tipo de Fraudes Informáticos.

Como medida de prevención y de protección, se han desarrollado una serie de medidas de seguridad que resguarden los sistemas bancarios y al cliente. Dentro de ellos se encuentra la criptografía o encriptación, el uso del protocolo SSL, los *Firewall* y antivirus, los IPS y los dispositivos físicos como las claves aleatorias, los Tokens y más recientemente los Certificados y Firmas Digitales. Además de la aplicación de estos sistemas, se recomienda una constante evaluación de riesgos y una política de concientización a los usuarios.

En el país no existe una ley específica que regule el tema de los delitos informáticos en la *Banca Online*. Los bancos basan sus medidas de seguridad en recomendaciones y buenas prácticas dadas a nivel nacional e internacional, pero ninguna es vinculante.

El perfil del consumidor de servicios informáticos en Costa Rica se caracteriza por una deficiencia en información y en conocimiento técnico sobre el uso correcto y seguro de las páginas WEB de los bancos, así como de las medidas de seguridad que deben tomar para protegerse adecuadamente contra los fraudes informáticos. Los Bancos no han brindado de forma correcta la capacitación necesaria para que el cliente interiorice los conceptos básicos y sea conciente de los riesgos que necesariamente se encuentran en este servicio. No se considera suficiente el dar dispositivos de seguridad al consumidor si

no se le explica adecuadamente su utilización, ventajas y riesgos, incluyendo así como medida de seguridad, además de la tecnología, la concientización y políticas de información y educación al cliente. Negarse a capacitar al cliente, o hacerlo de modo superficial provoca un riesgo que le es imputable a los Bancos.

Los consumidores usuarios de la Banca Estatal que han sido afectados por fraudes informáticos han acudido a los Tribunales de Justicia en busca de una solución y reparación. Los organismos de defensa de los derechos del consumidor se han hecho presentes en la representación de los intereses de este grupo de víctimas. La ACL elaboró el primer Proceso Colectivo en materia del consumidor que se encuentra en resolución el los Tribunales Contenciosos Administrativos.

Las sentencias existentes hasta hoy, tanto por el Tribunal Contencioso Administrativo como por la Sala Primera, han sostenido el criterio de responsabilizar objetivamente a los bancos por los riesgos encontrados en el servicio de Banca por Internet, específicamente en las medidas de seguridad utilizadas para la autenticación del cliente, la desinformación y el consecuente daño provocado. Los bancos se han opuesto tanto en sus contestaciones como en sus casaciones a este criterio, sin embargo, no ha sido modificado, salvo por un voto de Sala Primera que admite la causal eximente de responsabilidad de culpa de la víctima.

El criterio de imputación que establece la Responsabilidad Objetiva aplica para las relaciones que son contractuales, no únicamente dentro del marco de la responsabilidad extracontractual, ya que lo importante es el riesgo creado y el daño producido como resultado o materialización de ese riesgo, sin que se eximan de ello las situaciones que suceden dentro de una relación contractual.

Los Bancos se encuentran obligados a responder civilmente por los daños que surjan como resultado de su actividad, siempre y cuando se demuestre la existencia de un nexo causal entre la conducta y el daño. Queda la posibilidad de que las entidades bancarias demuestren que el daño fue ajeno cuando pruebe que existió alguna de las eximentes de culpabilidad que la ley establece. De este modo, los jueces deben realizar un análisis casuístico tomando en cuenta cada una de las pautas que configuran la responsabilidad para determinar si se debe o no responsabilizar a los bancos para el caso determinado.

La hipótesis entonces queda comprobada en el tanto se ha demostrado la existencia de Responsabilidad Objetiva en el tema en cuestión, con la posibilidad de exonerarse de responsabilidad cuando se comprueba la existencia de un eximente de responsabilidad, es decir, fuerza mayor, culpa de la víctima o hecho de un tercero. Se propone que los bancos brinden capacitaciones a los clientes, que se cree un reglamento

a nivel del Banco Central, la SUGEF o el CONASSIF con el fin de establecer una serie de medidas mínimas de seguridad con las que deben contar los bancos que pretenden brindar el servicio de banca por Internet, además de incluir mecanismos de capacitación que sean obligatorios para quienes deseen utilizar el servicio de Banca por Internet.

Es también importante que se revisen los contratos de adhesión elaborados por los bancos con el fin de eliminar cualquier cláusula abusiva que perjudique a los consumidores y constituya un abuso de poder. Asimismo, se considera necesario eliminar la presunción de culpabilidad que los bancos han incorporado dentro de sus reglamentos y que resulta contraria a los principios constitucionales y legales que benefician al consumidor, justamente con el fin de equilibrar la relación existente entre productor y consumidor es que se determinó conveniente utilizar el régimen de responsabilidad objetiva que conlleva una parcial inversión de la carga de la prueba para la víctima.

BIBLIOGRAFÍA

LIBROS

BAUZA REILLY, Marcelo. (1996). *Responsabilidad Civil en materia informática*. Informática y Derecho: II Congreso Internacional de Informática y Derecho. España. No. 9-10-11.

BOLOTNIKOFF, Pablo. (2004). *Informática y Responsabilidad Civil*. Buenos Aires, Argentina. La Ley S.A. PP. 371.

CHINCHILLA SANDÍ, Carlos. (2004). *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. San José, Costa Rica. Ediciones Farben. PP. 152.

FERNÁNDEZ LÁZARO, Fernando. (2007). *Los nuevos medios de investigación en el proceso penal: especial referencia a la tecnovigilancia. Medios técnicos en la Investigación de los Delitos Informáticos*. Madrid, España. Consejo General del Poder Judicial. PP. 191 Y 192.

GALLARDO MARTÍNEZ, Helio. (2008). *Elementos de investigación académica.* San José, Costa Rica. EUNED.

HABA MÜLLER, Enrique Pedro (1972). *Esquemas metodológicos en la interpretación del derecho escrito*. *Cuadernos de Filosofía del Derecho*. Caracas, Venezuela. Universidad Central de Venezuela.

LANCE, J. y STEWART J. (2005). *Phishing exposed, uncover secrets from the dark side*. Syngress Publishing, Inc.

LÓPEZ CABANA, Roberto (1995). *Responsabilidad Civil Objetiva.* Buenos Aires, Argentina. Editorial Abeledo-Perrot. PP. 255.

LUZ CLARA, Bibiana (2001). *Manual de Derecho Informático*. Rosario Santa Fe, Argentina. Nova Tesis Editorial Jurídica. PP. 160.

MAIWALD, Eric (2005). *Fundamentos de seguridad de redes*. México. Segunda edición. McGraw Hill Interamericana. PP. 475.

MARIE KNORR, Jolene y ROLDÁN SAUMA, Marcelo (2001). *La Protección del consumidor en el comercio electrónico.* San José, Costa Rica. Investigaciones Jurídicas S.A. PP. 282.

MÉNDEZ RAMÍREZ, Odilón. (1981). *La estructura formal de los trabajos finales de graduación*. San José, Costa Rica. Instituto de Investigaciones Jurídicas, Universidad de Costa Rica, Facultad de Derecho. PP. 65.

MONTERO PIÑA, Fernando. (1999). *Obligaciones*. San José, Costa Rica. Premiá Editores. PP. 360.

MORENO QUESADA, Bernardo y otros (1998). *Curso de derecho civil: contratos en particular, cuasicontratos y responsabilidad por hechos ilícitos*. Valencia, España. Editorial Tirant Io Blanch. PP. 526.

MOSSET ITURRASPE, Jorge. (1980). *Estudios sobre la responsabilidad por daños*. Santa Fe, Argentina. Editorial Rubinzal Culzoni. PP. 330.

MUGUILLO, Roberto A. (2006). *Responsabilidad de los bancos frente al cliente: Responsabilidad de la banca frente al usuario de tarjeta de crédito*. Buenos Aires, Argentina. Rubinzal Culzoni Editores.

OROZCO PARDO, Guillermo. (1998). *Responsabilidad Civil en materia de informática*. Jornadas marco legal y deontológico de la informática: actas volumen I. España. No. 19-20-21-22.

PÉREZ VARGAS, Víctor. (1994). *Derecho Privado*. San José, Costa Rica. Tercera Edición. Litografía e Imprenta LIL, S.A. PP. 514.

POUND, Roscue. (1954). *El Derecho como Ingeniería Social*. Edición Losada. Buenos Aires, Argentina.

RIVERO SÁNCHEZ, Juan Marcos. (1997). *¿Quo Vadis Derecho del Consumidor?*. Medellín, Colombia. Biblioteca Jurídica Diké.

RIVERO SÁNCHEZ, Juan Marcos. (2001). *Responsabilidad Civil*. Curso de Derecho Privado Tomo II. San José, Costa Rica. Segunda Edición. Ediciones Jurídicas Areté. Biblioteca jurídica Diké. PP. 367.

RODRÍGUEZ AZUERO, Sergio. (2002). *Contratos Bancarios: su significación en América Latina*. Colombia. Quinta edición. Legis Editores S.A.

SANABRIA ROJAS, Rafael Ángel. (2008). *Reparación civil en el proceso penal*. San José, Costa Rica. EDITORAMA S.A.

STIGLITZ, G. y STIGLITZ, R. (1994). *Derechos y defensa del consumidor*. Buenos Aires, Argentina. Ediciones La Roca. PP. 398.

REVISTAS

QUESADA ROMÁN, Carlos y CHACÓN SOLÍS, Esteban. *Transferencia Electrónica de fondos*. Revista Judicial N° 77, año XXIII, Corte Suprema de Justicia, San José, Costa Rica. PP. 33 a 73.

TRABAJOS FINALES DE GRADUACIÓN

BARRIENTOS NÚÑEZ, Greysa y VIETO HERNÁNDEZ, Nancy (1995). *Contratación de Bienes y Servicios Informáticos*. Tesis de grado para optar por el título de Licenciadas en Derecho. Universidad de Costa Rica, Facultad de Derecho.

GUERRERO MURILLO, Patricia y RODRÍGUEZ JIMÉNEZ, Karla (2001). *Derecho Informático Costarricense Sistematización y Análisis*. Tesis de grado para optar por el título de Licenciado en Derecho. Facultad de Derecho, Universidad de Costa Rica.

LÓPEZ CHAVARRI, José Francisco (2001). *Seguridad transaccional en la contratación electrónica privada*. Tesis de grado para optar por el título de Licenciado en Derecho Universidad de Costa Rica, Facultad de Derecho.

MORALES AVENDAÑO, Karla y FIGUEROA LOAIZA, Manuel (2003). *Formas Alternativas de Comercio Internacional: La Contratación electrónica y la seguridad jurídica transaccional*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho.

PORTELA ROJAS María y SOTO MORA, Catalina (2002). *Propuesta de Regulación del Comercio electrónico en Internet (Análisis a la Ley Modelo sobre comercio electrónico de la CNUDMI)*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho.

REYES VÁSQUEZ, Julio (2005). *El delito de Fraude Informático en Costa Rica*. Tesis de grado para optar por el título de Licenciado en Derecho .Universidad de Costa Rica, Facultad de Derecho

SOTO FONSECA, María Alejandra (1997). *La Responsabilidad Bancaria en la Transferencia electrónica de fondos*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho.

TREJOS ANTILLÓN, Oscar. (1996). *La Responsabilidad Civil en las transferencias electrónicas de información: necesidad de una legislación sobre la transferencia bancaria*. Tesis de grado para optar por el título de Licenciado en Derecho. Universidad de Costa Rica, Facultad de Derecho.

CONSTITUCIÓN, LEYES Y REGLAMENTOS

Constitución Política de la República de Costa Rica de 7 de noviembre de 1979. San José, Costa Rica. Editorial Investigaciones Jurídicas S.A. 2005.

Código Civil, Ley N° 30 de 19 de abril de 1885.

Código Procesal Contencioso Administrativo, Ley N° 8508 del 28 de abril de 2006.

Ley de Certificados, Firmas Digitales y documentos electrónicos, Ley N° 8454 del 30 de agosto del 2005.

Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley N° 7472 de 20 de diciembre de 1994.

Ley Orgánica del Sistema Bancario Nacional, Ley N° 1644 del 25 de setiembre de 1953.

Proyecto de Ley de Comercio Electrónico, Expediente Legislativo 16081.

Proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales, Expediente Legislativo 16679.

Reglamento a la Ley de certificados, firmas digitales y documentos electrónicos, N° 33018 del 20 de marzo de 2006.

Reglamento del Sistema de Pagos, aprobado por la Junta Directiva del Banco Central de Costa Rica en la sesión 5368-2008, publicado en el diario oficial La Gaceta 53 del 14 de marzo del 2008.

Reglamento sobre la gestión de la tecnología de información (2009), acuerdo SUGEF 14-09, publicado en el diario oficial La Gaceta 50 del 12 de marzo del 2009.

Reglamento de Servicios de Banca Electrónica del Banco de Costa Rica (2004), acuerdo Junta Directiva en sesión 10-04, publicado en el diario oficial La Gaceta 81 del 16 de marzo del 2004.

Normas técnicas para la gestión y control de las Tecnologías de Información, Contraloría General de la República. N-2-2007-CO-DFOE, publicadas en el diario oficial La Gaceta 119 del 21 de junio del 2007.

Código de autorregulación de buenas prácticas bancarias para la protección de las transacciones efectuadas mediante el uso de instrumentos electrónicos de pago. Cámara de Bancos e instituciones financieras de Costa Rica. S.f.

Directrices de la ONU para la protección del consumidor. Naciones Unidas Resolución A/RES/39/248 del 16 de abril de 1985.

JURISPRUDENCIA

Sala Constitucional de la Corte Suprema de Justicia. Voto N° 1441-92 de las quince horas cuarenta y cinco minutos del dos de junio de mil novecientos noventa y dos.

Sala Primera de la Corte de Justicia. Sentencia 61-1997 de las catorce horas cincuenta minutos del diecinueve de junio de mil novecientos noventa y siete.

Sala Primera de la Corte Suprema de Justicia. Sentencia 376-F-99 de las catorce horas cuarenta minutos del nueve de julio de mil novecientos noventa y nueve

Sala Primera de la Corte Suprema de Justicia. Sentencia 00460-F-2003 de las diez horas cuarenta y cinco minutos del treinta de julio del dos mil tres.

Sala Primera de la Corte Suprema de Justicia. Sentencia 00654-04 de las once horas con cincuenta minutos del cinco de agosto del dos mil cuatro.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000295-F-2007 de las diez horas cuarenta y cinco minutos del veintiséis de abril del dos mil siete.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000467-F-S1-2008 de las catorce horas veinticinco minutos del cuatro de julio de dos mil ocho.

Sala Primera de la Corte Suprema de Justicia. Sentencia 00300-F-S1-2009 de las once horas con veinticinco minutos del veintiséis de marzo del dos mil nueve.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000394-F-S1-2009 de las diez horas veinte minutos del veintitrés de abril del dos mil nueve.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000395-F-S1-2009 de las diez horas veinticinco minutos del veintitrés de abril del 2009.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000396-F-S1-2009 de las diez horas treinta minutos del veintitrés de abril del 2009.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000397-F-S1-2009 de las diez horas treinta y cinco minutos del veintitrés de abril de dos mil nueve.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000398-F-S1-2009 de las diez horas cuarenta minutos del veintitrés de abril del 2009.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000399-F-S1-2009 de las diez horas cuarenta y cinco minutos del veintitrés de abril del dos mil nueve.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000827-F-S1-2009 de las ocho horas del siete de agosto del dos mil nueve.

Sala Primera de la Corte Suprema de Justicia. Sentencia 000516-F-S1-2009 de las diez horas veinte minutos del veintisiete de mayo del dos mil nueve.

Sala Tercera de la Corte Suprema de Justicia. Sentencia 00535-2004 de las nueve horas con cinco minutos del veintiuno de mayo de dos mil cuatro.

Sala Tercera de la Corte Suprema de Justicia. Sentencia 00383-2005 de las ocho horas cuarenta minutos del trece de mayo del dos mil cinco.

Sala Tercera de la Corte Suprema de Justicia. Sentencia 117-2005 de las dieciséis horas con veinticinco minutos del veintinueve de setiembre del dos mil cinco.

Sala Tercera de la Corte Suprema de Justicia. Sentencia 148-2006 de las nueve horas del veinticuatro de febrero del dos mil seis.

Sala Tercera de la Corte Suprema de Justicia. Sentencia 01333-2007 de las diez horas con quince minutos del dos de noviembre del dos mil siete.

Tribunal de Casación Penal. Sentencia 0493-2004 de las diez horas con once minutos del veinte de mayo del dos mil cuatro.

Tribunal de Casación Penal. Sentencia 00608-2008 de las nueve horas con quince minutos del veintiséis de mayo del dos mil ocho.

Tribunal de Casación Penal. Sentencia 0840-2008 de las catorce horas con quince minutos del veinticinco de agosto del dos mil ocho.

Tribunal de Casación Penal. Sentencia 00617-09 de las diez horas quince minutos del doce de junio del dos mil nueve.

Tribunal Agrario del Segundo Circuito Judicial de San José. Sentencia 00815-2003 de las catorce horas y cincuenta y cinco minutos del dieciséis de diciembre del dos mil tres.

Tribunal Primero Civil de San José. Sentencia 668-F-08 de las siete horas treinta minutos del ocho de agosto del dos mil ocho.

Tribunal Segundo Civil, Sección Primera. Sentencia 035-2009 de las nueve horas cuarenta minutos del veintiuno de enero de dos mil nueve.

Tribunal Segundo Civil, Sección Segunda. Sentencia 258-2009 de las dieciséis horas cincuenta minutos del treinta y uno de julio del dos mil nueve.

PÁGINAS WEB

Asociación de Consumidores Libres (2009). <http://www.consumidoreslibres.org/index.htm>. [Consulta del 02 de noviembre del 2009].

Banco de Costa Rica (2009). <http://www.bancobcr.com>. [Consulta del 23 de noviembre de 2009].

Banco Nacional (2009). <http://www.bncr.fi.cr>. [Consulta del 23 de noviembre de 2009].

Banco Popular (2009). <https://www.popularenlinea.fi.cr/Bpop/>. [Consulta del 23 de noviembre de 2009].

BAC San José (2009). <https://www.bac.net/bacsanjose/esp/banco/index.html>. [Consulta del 23 de noviembre de 2009].

BISCIONE, Carlos (2009). *Ingeniería social para no creyentes.* <http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf>. [Consulta del 24 marzo de 2009].

CISCO Networking Academy (2009). <http://www.cisco.com/web/learning/netacad/index.html>. [Consulta del 4 diciembre 2009].

Consumidores de Costa Rica (2009). <http://www.consumidoresdecostarica.org/informacion_general.html>. [Consulta del 02 de noviembre del 2009].

HSBC Costa Rica (2009) <http://www.hsbc.fi.cr/a/bp/banca_por_internet.asp>. [Consulta del 23 de noviembre de 2009].

FERNÁNDEZ PALMA, Rosa (2006). *Reseña de la Jornada sobre los riesgos penales de la banca on-line*. <http://www.uoc.edu/idp/2/dt/esp/fernandez.pdf.> [Consultada el 25 de noviembre de 2009].

PAGET, François (2007).*Robos de Identidad*. Mc Afee Avert Labs. <www.mcafee.com> [visitado el 02 de Octubre de 2009].

SALAZAR SOLÓRZANO, Randall (S.F.). La Tutela Constitucional del consumidor. Instituto de Investigaciones Jurídicas, Facultad de Derecho de la Universidad de Costa Rica.<http://www.iij.derecho.ucr.ac.cr/archivos/documentacion/derecho%20del%20consumidor/La%20Tutela%20Constitucional%20del%20Consumidor.pdf>. [Visita realizada el 10/02/10].

SMART CARD (2009). <www.smart-card.com/.../smart-card-security.jpg>. [Consulta del 08 de diciembre de 2009]

Superintendencia General de Entidades Financieras, SUGEF. (2009). <http://www.sugef.fi.cr/pagina.asp?lang=0&pagina=servicios/documentos/infgeneral/funciones/SUGEF.pdf> [consultada el 27 de noviembre de 2009]

The complete social engineering faq! (2009). Traducción moderada. <http://packetstorm.linuxsecurity.com/docs/social-engineering/socialen.txt>. [Consulta del 25 marzo de 2009].

Wikipedia (2009).< http://es.wikipedia.org/wiki/Hipertexto>. [Consulta del 27 de noviembre de 2009].

Wikipedia (2009). <http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos>. [Consulta del 29 de noviembre de 2009].

Wikipedia (2009). <http://es.wikipedia.org/wiki/Sistema_de_Prevenci%C3%B3n_de_Intrusos>. [Consulta del 29 de noviembre de 2009].

Wikipedia (2009). <http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)>. [Consulta del 29 de noviembre de 2009].

Wikipedia (2009). <http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)>. [Consulta del 29 de noviembre de 2009].

Wikipedia (2009). <http://es.wikipedia.org/wiki/Archivo:Gateway_firewall.svg>. [Consulta 29 de noviembre de 2009].

ARTÍCULOS

PÉREZ VARGAS, Víctor (2008, 13 de enero). Fraudes Informáticos. Periódico La Nación, Opinión. P. 15.

CONGRESOS, SEMINARIOS, SIMPOSIOS, TALLERES

CHINCHILLA SANDÍ, Carlos y CHIRINO SÁNCHEZ, Alfredo. (2009). *"Delitos Informáticos: Necesidad de nuevas formas de regulación".* Mesa Redonda. Colegio de Abogados. San José, Costa Rica. 25 de noviembre de 2009.

IX Jornadas de AUSBANC Internacional (2009). *"Nuevos Derechos Financieros del Siglo XXI"*. Mesas Redondas. Colegio de Abogados. San José, Costa Rica. 01 y 02 de octubre de 2009.

ENTREVISTAS

ALVARADO, Max (2009). Ingeniero en Sistemas. Entrevista en CISCO Systems, Plaza Roble. 06 de octubre de 2009.

BRENES VILLALOBOS, Rafael (2009). Abogado Banco Nacional. Entrevista en el Banco Nacional de Costa Rica, sede central. 01 de setiembre de 2009.

CUADRA CHAVARRÍA, William (2009). Ingeniero informático Banco Nacional. Entrevista en Banco Nacional de Costa Rica, sede central. 16 de setiembre del 2009.

LACAYO, Raúl (2009). Jefe de Seguridad del Banco Popular. Chat a través de nacion.com del 23 de noviembre del 2009 a las 09:00 a.m.

RAMÍREZ ALFARO, Manuel (2009). Ingeniero Informático del Banco Popular. Entrevista realizada vía correo electrónico. 19 de octubre del 2009.

RAMÍREZ CASTRO, Eduardo (2009). Director Jurídico Banco de Costa Rica. Entrevista en el Banco de Costa Rica, sede central. 17 de noviembre de 2009.

ROJAS RIVERO, Adriana (2009). Abogada Asociación de Consumidores Libres. Entrevista en la oficina de la ACL, San José. 25 de agosto de 2009.

SEBIANI SERRANO, Alejandro (2009). Gerente de Seguridad en Tecnología del Banco de Costa Rica. Entrevista Sucursal Banco de Costa Rica, Barrio Aranjuéz. 14 de setiembre de 2009.

ANEXOS

1. ENCUESTA REALIZADA

ENCUESTA
EL SERVICIO DE BANCA POR INTERNET

Esta información será utilizada únicamente para fines académicos, se garantiza su total confidencialidad.

DATOS PERSONALES

- Sexo: Masculino ( ) Femenino ( )
- Rango de edad:
  ( ) 18 a 30
  ( ) 30 a 40
  ( ) 40 en adelante
- Educación:
  Primaria: completa ( ) incompleta ( )
  Secundaria: completa ( ) incompleta ( )
  Universitaria: completa ( ) incompleta ( )
  Post grados: _____
  Técnico: _____
- A qué se dedica: _____

CUESTIONARIO

1. ¿Es usted usuario de la Banca Electrónica? Si su respuesta es negativa no continúe la encuesta.
   ( ) Sí
   ( ) No

2. Utiliza los servicios de Banca por Internet de:
   ( ) Banca Estatal
   ( ) Banca Privada
   ( ) Ambas

3. ¿Desde cuándo es usted cliente de la Banca Electrónica?
   _____

4. Marque el (los) tipo(s) de transacción(es) que realiza en la página de Banca por Internet de su entidad bancaria
   ( ) Pago de servicios públicos
   ( ) Pagos universitarios
   ( ) Transferencias a otras cuentas del mismo Banco
   ( ) Transferencias entre cuentas de diferentes bancos por medio del SINPE
   ( ) Otro, especifique_____

5. ¿Tiene algún cuidado especial cuando realiza transacciones por Internet?
   ( ) Sí, cuáles_____
   ( ) No

6. ¿En qué lugar (es) accede a la página del Banco en que realiza sus transacciones?
   ( ) Casa
   ( ) Trabajo
   ( ) Café Internet
   ( ) Otros, especifique:_____

7. ¿Se asegura que el equipo que utiliza para hacer uso del servicio de banca en línea cuente con dispositivos de seguridad tales como
   ( ) antivirus actualizado
   ( ) Anti-Spyware
   ( ) Firewall
   ( ) Otros
   ( ) No
   - Si su respuesta es afirmativa en cuanto al antivirus, sabe si el que posee fue adquirido
     ( ) de manera gratuita
     ( ) compró la licencia
     ( ) no sabe

   - Si su respuesta es Negativa pase a la pregunta 10.

8. ¿Se encuentra usted pendiente de mantener actualizado su antivirus?
( ) Sí
( ) No

9. ¿Realiza usted con frecuencia revisiones a su computadora para comprobar que se encuentre libre de virus y demás amenazas?
( ) Sí
( ) No

10. ¿Sabe usted que características tiene una página de Internet catalogada como un sitio seguro de una que no lo es?
( ) Sí
( ) No

Si su respuesta es afirmativa detalle cuáles son esas características que usted distingue: _____
_____

11. ¿Utiliza usted la opción de "recordar contraseña" para sus visitas a sitios de Internet?
( ) Sí
( ) No

12. ¿Ha recibido de alguna manera por parte del Banco de su elección algún tipo de capacitación para utilizar el servicio de banca electrónica de manera segura?
( ) Sí, Especifique_____
( ) No

13. ¿Ha revisado en las páginas de Internet del Banco que utiliza algún tipo de consejos y/o demos de las prácticas recomendadas para el uso de forma segura de la Banca Electrónica?
( ) Sí
( ) No

14. Marque, si sabe en lo que consiste, cualquiera de las siguientes conceptos:
( ) Phishing
( ) Pharming
( ) Troyanos
( ) Spyware
( ) Malware

15. ¿Ha sido usted víctima de algún tipo de delito informático?
( ) Sí
( ) No

16. ¿Su banco le ofrece algún tipo de dispositivo de seguridad además de su clave de acceso?
( ) Sí, Cuál _____
( ) No
Si su respuesta es negativa pase a la pregunta 19.

17. ¿Hace uso usted de este tipo de dispositivos?
( ) Sí
( ) No

18. ¿Para cuáles transacciones le solicita su Banco la utilización de este tipo de Dispositivos?
    ( ) Pago de servicios públicos
    ( ) Pagos universitarios
    ( ) Transferencias a otras cuentas del mismo Banco
    ( ) Transferencias entre cuentas de diferentes bancos por medio del SINPE
    ( ) Otro, especifique_____

19. ¿Cómo calificaría el nivel de seguridad que le brinda su Banco para el servicio de Banca Electrónica?
( ) Excelente
( ) Muy bueno
( ) Bueno
( ) Malo
( ) Muy malo

¡Muchas gracias por su colaboración!

2. NOTICIA: "PRÁCTICAS DE BANCA EN LÍNEA EN COSTA RICA SON INACEPTABLES"

Costa Rica, Miércoles 13 de febrero de 2008
nacion.com /EL PAÍS

BANCOS INCUMPLEN MEJORES ESTÁNDARES INTERNACIONALES

Prácticas de banca en línea en Costa Rica son inaceptables

- Bancos en exterior tienen que probar culpa de cliente o reintegrar el dinero
- Superintendente recomienda aplicar una medida similar en Costa Rica

HAZEL FEIGENBLATT | hfeigenblatt@nacion.com

Los bancos costarricenses someten a los usuarios de los servicios bancarios por Internet a prácticas inaceptables en países desarrollados.

No hay ninguna ley o institución pública que los obligue a responder ante sus clientes por fraudes electrónicos, y ello les ha dado libertad para negarse a aceptar responsabilidades que sus similares en otros países sí aceptan.

MÁS SOBRE ESTE TEMA
Víctimas no tienen a nadie a quién acudir
"Nuestros expertos nos tienen tranquilos"
Abogada ya tiene lista demanda contra banco
Empresario sospecha que hubo 'gato casero'
La palabra del banco contra la del cliente
Imprimir Recomendar
Disminuir Aumentar

Aquí los bancos se niegan a reintegrar el dinero robado electrónicamente y les basta con decir que probablemente el fraude ocurrió por descuido del usuario.

Ello es inaceptable en Estados Unidos, en donde el banco debe reintegrar el dinero o probar que el usuario actuó fraudulentamente o incurrió en un descuido.

Aunque aquí los bancos dicen cumplir los estándares internacionales de seguridad, muchos operan con solo un mecanismo de verificación de identidad.

Eso también es inaceptable en Estados Unidos, donde desde el 2005 las cinco autoridades financieras calificaron tal práctica como "inadecuada", y actualmente no la permiten si es el único medio de autenticación.

Adicionalmente, expertos informáticos afirmaron a *La Nación* que cada vez hay más formas de robar la información bancaria hasta a los usuarios más cautos, y creen desproporcionado asignarle todo el riesgo al cliente.

Carga de la prueba. Hay casi 500 denuncias de fraude electrónico, con pérdidas por más de ¢800 millones, y los bancos se niegan a reintegrar el dinero.

Ello difiere dramáticamente de Estados Unidos, donde la ley ordena que el banco reintegre el dinero o pruebe que el usuario actuó de forma fraudulenta, o que de alguna forma permitió que la transferencia se realizara.

El presidente de la Asociación Bancaria Costarricense, Mario Castillo, dijo: "(A los bancos) no se les puede pedir que sean responsables de algo por lo que no fueron responsables". Agregó que hay un vacío legal y que la Asociación está dispuesta a colaborar en un eventual proyecto de ley.

La ausencia de ley no fue excusa para los banqueros ingleses, quienes voluntariamente crearon el Código Bancario. Este incluye una norma similar a la de EE. UU.

Consultado sobre qué está haciendo la Superintendencia de Entidades Financieras (Sugef) al respecto, el superintendente, Óscar Rodríguez, dijo que esta no tiene potestad legal para intervenir.

Sí opinó que en Costa Rica debe hacerse una ley para que se aplique el mismo principio que en esos países. "Sería un incentivo muy poderoso para que los bancos eleven los niveles de seguridad", dijo.

Añadió que hoy algunos bancos están "mucho más preparados" que otros en materia de seguridad, pero que tiene prohibición legal para revelar los detalles.

¿Los mejores estándares? Un argumento de los bancos costarricenses para rechazar los reclamos de los clientes perjudicados es que sus sistemas de seguridad cumplen los estándares internacionales.

No obstante, aquí numerosos bancos aplican solo un mecanismo de verificación de identidad del usuario (por ejemplo, número de cédula y palabra clave).

Desde octubre del 2005, las cinco entidades financieras estadounidenses advirtieron que ese mecanismo es "inadecuado".

"El fraude bancario y el robo de identidad son frecuentemente resultado de la explotación de sistemas de verificación de un factor (número de identidad y palabra clave)", afirma una guía de acatamiento obligatorio emitida por el Consejo de Revisión de Instituciones Financieras Federales.

La Oficina de Prensa de la entidad confirmó a *La Nación* que actualmente no se permite que los bancos operen de esa forma.

Un ejemplo de un banco que opera así en Costa Rica es el Banco Nacional, el cual tiene más clientes y también más casos de fraude.

Al cierre, no se recibió respuesta del gerente, William Hayden.

Ofrecen un segundo mecanismo de verificación HSBC, BAC San José (aunque es opcional y con un costo extra) y, recientemente, el Banco de Costa Rica (BCR).

El subgerente del BCR, Mario Rivera, aseguró que desde diciembre se han entregado 25.000 "claves dinámicas" y ninguno de esos usuarios ha sufrido fraude.

Luis Lieberman, gerente de Scotiabank, afirmó que pronto lanzarán un segundo mecanismo y Banca Promérica lo ofrece solo para algunos clientes.

Riesgo. Roberto Sasso, presidente del Club de Investigación Tecnológica, dijo que, aún con los mejores sistemas de seguridad, ninguna transacción por Internet es 100% segura. Estimó "desproporcionado" que todo el riesgo de la banca en línea lo tenga que asumir la parte contractual más débil: el usuario.

Carlos Melegatti, responsable del Sistema Nacional de Pagos Electrónicos (Sinpe), del Banco Central, comentó que esa entidad no tiene injerencia sobre los bancos. No obstante, coincidió con Sasso y recomendó hacer una reforma legal. "Los sistemas injustos no tienen futuro", advirtió.

FOTOS

ampliar

ROBO DE CLAVES A USUARIOS CAUTOS

Pharming

Se altera un servidor (por ejemplo, el de su trabajo) para que cuando usted escriba la dirección de su banco sea llevado a la de un sitio web falso que parece el de banco. Ello lo puede hacer un virus nuevo o incluso la persona a quien usted le confía hacer esas cosas "técnicas" en su computadora.

Sniffers

Es un programa que se instala en una computadora y "observa" todo (hasta datos bancarios) lo que pasa por el segmento de la red que la máquina comparte con otras (por medio de un cable coaxial o de fibra óptica). Es decir, "observa" las demás computadoras. Los antivirus y "antispyware" reducen el riesgo, no lo elimina.

Robots

Un virus instala un programa en su computadora y le da control remoto sobre esta al criminal, que no solo puede obtener sus claves sino hasta hacer transacciones desde su computadora. Se han descubierto "ejércitos de computadoras zombies" de hasta medio millón de ordenadores.

Keyloggers

Es un virus que se puede obtener con tan solo visitar un sitio web (incluso no bancario), el cual abre un programa que registra lo que usted teclea y se lo envía al criminal. Aunque los antivirus disminuyen el riesgo, estos son posteriores a la creación del virus.

ADEMÁS EN EL PAÍS
Atraso de acta impidió votación de Ley de Telecomunicaciones
Confusión por nombramiento de maestras en escuela Gamonales
Diputados aprueban Ley General de Telecomunicaciones
Sala IV frena construcciones en parque Las Baulas
Diez colegios perdieron subvención del Estado

De momento, los bancos no tienen que rendir cuentas a nadie. *La Nación* envió preguntas a varios. El BAC San José dijo que es "imposible" dar la información. No respondieron: HSBC, Popular, Banco Uno, Aval Card, Improsa y Cathay.

3. NOTICIA: "BANCO NACIONAL RECIBE PRIMERA CONDENA POR FRAUDE EN LÍNEA"

Costa Rica, Viernes 10 de octubre de 2008
nacion.com /el país

SAQUEO DE CUENTA BANCARIA POR INTERNET

Banco Nacional recibe primera condena por fraude en línea

- Joven universitario demandó para recuperar ¢1,1 millones
- BN estudiará 'en detalle' la sentencia y valora acudir a otras instancias para apelar

HAZEL FEIGENBLATT | hfeigenblatt@nacion.com

El Banco Nacional (BN) fue condenado ayer por primera vez a reintegrarle el dinero a un cliente que fue víctima de fraude por Internet.

La demanda fue planteada por el estudiante universitario Cristian Loría, quien el año pasado perdió ahorros por ¢1,1 millones que pensaba utilizar para terminar su licenciatura en Administración de Negocios.

Imprimir · Recomendar · Disminuir · Aumentar

"Yo sabía que se tenía que hacer justicia. Se sentó un precedente y puede beneficiar a otras personas que están en la misma situación", comentó Loría ayer tras escuchar la sentencia.

Se trata de la tercera condena contra un banco costarricense por el tema de fraudes electrónicos, luego de que el Banco de Costa Rica (BCR) recibió dos sentencias similares en setiembre.

En el país hay unas 500 víctimas de este delito, en su mayoría clientes del BN y del BCR.

Hay otras 10 demandas en proceso contra ambas entidades y una de ellas representa a más de 120 personas, reunidas por la Asociación de Consumidores Libres, a la cual aún se pueden agregar más personas.

Ayer, la Oficina de Prensa del BN dijo: "El Banco Nacional respeta pero no comparte el fallo del Tribunal. Estudiará en detalle la sentencia, tanto por la forma como por el fondo, para definir si acude a otras instancias. Es una posibilidad que está valorando".

En contraste, el BCR dijo hace algunos días que analiza la posibilidad de no apelar las dos condenas recibidas e, incluso, podría conciliar con algunos clientes.

Responsabilidad. En el Banco Nacional se han reportado al menos 278 casos y la entidad ha rechazado los reclamos de los perjudicados, pues estima que el acceso a la cuenta del cliente ocurre solo si este, de alguna manera, lo facilitó.

No lo ven así los tribunales.

Los tres jueces del Tribunal Contencioso Administrativo determinaron de forma unánime que el BN tuvo responsabilidad objetiva por lo ocurrido.

Según la ley, un proveedor puede ser responsable si el consumidor resulta perjudicado en razón de las características propias del bien o servicio brindado, independientemente de que tenga culpa o no.

El abogado demandante, Guido Granados, afirmó que en el juicio se demostró que el Banco Nacional no tomó medidas de seguridad que podían evitar los fraudes.

La Nación publicó en febrero que bancos como el BN y el BCR tuvieron sus plataformas electrónicas con solo un mecanismo de autenticación de identidad, pese a que desde el 2005 se conocía que ello era inadecuado e inseguro.

Según Granados, quedó demostrado que el BN fue alertado de ese hecho en un informe interno y no tomó ninguna decisión, sino hasta finales del 2007, cuando ya se habían producido cientos de fraudes.

Medidas de seguridad. "El Banco acudió a la Contraloría para que le autorice una contratación de urgencia (para poner un mecanismo de doble autenticación de identidad) y ahí dice que es por inseguridad del sistema", afirmó Granados. "Si lo hubiesen hecho en el 2005, no hubiera pasado nada", agregó.

El BN respondió ayer: "Los casos se empezaron a presentar en Costa Rica en el 2007, y en ese mismo año el Banco Nacional tomó medidas adicionales para proteger a los clientes, como fue la restricción de transferencias solo a cuentas favoritas".

Sobre la medida de poner topes al monto que podía ser transferido electrónicamente, Granados dijo que en el juicio se demostró que, en el caso de Loría, el tope no impidió el fraude. "El Banco nunca le dijo (a Loría) que ese tope no servía para nada", comentó.

Con esta sentencia queda claro que la política aplicada hasta ahora por los bancos no se ajusta al marco legal del país.

Pese a ello, ninguno ha anunciado un cambio de política. En la práctica, esto significa que se les traslada la responsabilidad de resolver, caso por caso, a los jueces contencioso-administrativos.

La Nación intentó conocer la posición de la Cámara de Bancos e Instituciones Financieras y de la Asociación Bancaria Costarricense sobre la primera sentencia contra el BN, pero no respondieron.

El BCR puso doble autenticación en diciembre del año pasado, y el BN, apenas el mes pasado.

El abogado Guido Granados y su cliente, el universitario Cristian Loría (de camisa azul), recibieron la sentencia con aspecto. Granados llevó el caso porque Loría trabaja en su bufete. Mario López

NUEVO SISTEMA REDUCE DURACIÓN DE PROCESOS

DEMANDA SE PROCESÓ EN 10 MESES

Aunque muchas demandas tardan años en resolverse en los tribunales, la demanda contra el Banco Nacional solo requirió 10 meses para llegar a una sentencia.

Algo similar ocurrió con las dos demandas planteadas contra el Banco de Costa Rica y ello se debe al nuevo Código Procesal Contencioso Administrativo, que empezó a regir este año.

La nueva normativa da a los jueces más herramientas para obligar a las instituciones públicas a corregir actuaciones o, incluso, a actuar ante sus omisiones.

La demanda y la contestación de la parte demandada son escritas, pero otras fases del proceso se resuelven en audiencias frente al juez, para las cuales se puede citar a las partes mediante recursos tecnológicos más ágiles.

El abogado que planteó la demanda contra el Banco Nacional, Guido Granados, comentó que le gustó el nuevo sistema porque, aun cuando el banco intentó "jugar" con el papeleo, los jueces podían ponerle plazos.

"Por ejemplo, para aportar una traducción, le dieron un máximo de tres días. Para otro documento le dieron 24 horas (...). Ahora sí se siente que hay justicia oportuna", comentó. Falta ver cuánto tiempo duraría en resolverse la apelación, si el Banco la presenta.

El nuevo código también da legitimación procesal a quienes invocan la defensa de intereses difusos (que afectan a todos los usuarios de la banca) o colectivos (a un número específico de usuarios).

Ello permitió a la Asociación de Consumidores Libres presentar una demanda colectiva –en representación de más de 120 víctimas de fraude por Internet– contra los bancos Nacional, de Costa Rica y Popular.

La demanda se presentó en junio y actualmente se encuentra en proceso.

ADEMÁS EN EL PAÍS
Inmigrantes dejan de ser una carga para la CCSS
Aplazado hasta enero del 2009 concurso para buses Interlínea
Restaurantes y bares, reacios a prohibir fumado

4. NOTICIA: “BCR CONDENADO A REINTEGRAR DINERO DE FRAUDE POR INTERNET A CLIENTE”

Costa Rica, viernes 28 de noviembre de 2008

nacion.com /el país

LN LL PAÍS

Buscar Búsqueda avanzada

PORTADA | EL PAÍS | DEPORTES | SUCESOS | ECONOMÍA | ALDEA GLOBAL | EL MUNDO | OPINIÓN | ENTRETENIMIENTO | CLASIFICADOS

Sociedad | Política | Su cantón

JUECES CONSIDERARON QUE EL BANCO NO OFRECÍA SUFICIENTE SEGURIDAD

BCR condenado a reintegrar dinero de fraude por Internet a cliente

- BCR descartaría apelar decisión y no deshecha posibles conciliaciones
- Más de 120 personas tienen demandas similares en proceso

[illegible] | [illegible]@nacion.com

El Tribunal Contencioso Administrativo y Civil de Hacienda condenó el viernes al Banco de Costa Rica (BCR) a reintegrar el dinero a una clienta que fue víctima de fraude bancario por Internet, dos veces el año pasado.

El BCR confirmó que es la primera sentencia que se produce en el país contra un banco por negarse a reponer el dinero desaparecido por vía electrónica.

MÁS SOBRE ESTE TEMA

Demandante molesta por manipulación en el juicio

El banco sí está preocupado

Imprimir | Recomendar | Disminuir | Aumentar

Cuatro demandas más están en proceso contra el BCR, una de las cuales se resolverá esta semana y otra que cubre reclamos de 120 usuarios.

En total, en ese banco se han presentado 250 fraudes.

Menos estricto. Para el Tribunal, quedó demostrado que el sistema de seguridad del BCR no fue suficientemente seguro, pues era "más estricto hacia lo interno del banco que hacia afuera". La parte externa se refiere a los mecanismos de seguridad para permitir el acceso por Internet a las cuentas.

Una investigación de este diario reveló en febrero que la mayoría de bancos en Costa Rica, entre ellos el BCR, lanzó el servicio de banca en línea con solo un mecanismo de autenticación de identidad, pese a que desde el 2005 las autoridades financieras de Estados Unidos habían advertido que ello es inadecuado e inseguro.

Un [illegible], debía ser objeto de particular atención (por parte del banco) ofrecer a sus clientes la suficiente seguridad para evitar los previsibles y reiterados ataques de delincuentes cibernéticos", dijeron los jueces Roberto Gutiérrez Brenes, Ana Isabel Vargas Vargas y Joaquín Villalobos Solís.

"Al no hacerlo o hacerlo tardíamente, el hecho de estos terceros (los ladrones) no permite eximir al banco de su clara responsabilidad", agregaron.

Fue hasta a finales del 2007 que el BCR ofreció un segundo sistema de verificación de identidad llamado Clave Dinámica.

Casi un año después, ni un solo usuario de la Clave Dinámica ha sido víctima de fraude, y desde el 17 de este mes su uso es obligatorio para todos los clientes del banco.

La sentencia indica que la seguridad requiere de actualización constante y debe ser extremada, pues ella "colabora para minimizar el riesgo que deriva del servicio de banca electrónica, catalogado como 'riesgoso' per se".

Cambio de actitud. Aunque el BCR venía la política de rechazar los reclamos, abrir el gerente, Mario Rivera, dijo que la entidad "no tiene definido si va a presentar recurso de casación", y que no descarta [illegible] conciliaciones.

Explicó que por ser una entidad del Estado, el banco consideraba estar sujeto a la *Ley general de la Administración pública* y no a la *Ley de protección y defensa efectiva del consumidor*, pero que será respetuoso de los fallos.

Sobre cómo se tratarán otros reclamos, dijo que "el Banco no puede ignorar los precedentes que se emitan" en estas primeras sentencias.

El fallo ordena al BCR a reintegrarle a Arroyo $4.979 y ¢1,4 millones, más los intereses y las costas procesales.

"Yo dejé mi plata en un banco, no en una alcancía. Tal vez no sea mucha plata, pero yo confío en el sistema judicial costarricense y había que sentar un precedente", comentó la demandante.

Hasta ahora los bancos han rechazado los reclamos de sus clientes con base en la suposición de que su sistema es muy seguro y de que si hay un fraude de alguna manera es por culpa del usuario.

Carga invertida. No obstante, los jueces advirtieron que no se puede invertir la carga de la prueba y que es a los bancos a quienes les corresponde probar que no son responsables del incidente.

El BCR no solo no pudo probar que la parte externa de su sistema hubiera sido suficientemente segura, sino que tampoco pudo probar que su clienta fuera descuidada con las claves.

Por ello, el tribunal consideró que los argumentos del banco "caen por su propio peso" y que aplica la responsabilidad objetiva, según la cual un proveedor es responsable si el consumidor resulta perjudicado en razón del bien o servicio, independientemente de que tenga culpa o no.

FOTOS

Marielos Arroyo, dueña de la empresa de alquiler y venta de vestidos Mussel, dijo que acudió a los tribunales porque dejó su dinero "en un banco, no en una alcancía", y porque "había que sentar un precedente". Jorge Castillo

VIDEOS

Vea el testimonio de la demandante.

Otros videos:

- Marielos Arroyo cuenta cómo en el juicio los abogados del BCR dieron que ella veía al banco como "una piñata"
- La demandante se queja del trato que le dieron cuando presentó el reclamo ante el BCR.

¿PRIMERO DE MUCHOS EN LOS?

DECISIÓN TRASCENDENTE

Los tres jueces aclararon en la sentencia lo siguiente: "No es ajeno a este Tribunal la trascendencia que este fallo encierra; sin embargo, consideramos que se debe resolver conforme a los hechos y el derecho vigente, sin estimar cuestiones puramente extrajurídicas esbozadas por la representación del Banco en su discurso de conclusiones". Los factores extrajurídicos se refieren al temor de los bancos de que si se les obliga a reintegrar el dinero podrían empezar a surgir casos de personas que se pongan de acuerdo con otras para simular que fueron víctimas de un fraude. Además, temen que se genere miedo en torno al uso de la banca electrónica, según explicó a *La Nación* el director jurídico del BCR, Eduardo Ramírez. En otros países los bancos están obligados a reintegrar el

5. NOTICIA: “CLIENTES BANCARIOS INDEFENSOS ANTE SAQUEO ELECTRÓNICO”

nacion.com /EL PAÍS

PORTADA EL PAÍS DEPORTES SUCESOS ECONOMÍA ALDEA GLOBAL EL MUNDO OPINIÓN ENTRETENIMIENTO CLASIFICADOS

Sociedad | Política | Su cantón | Pulso diario

PÉRDIDAS PASARON DE ¢52 MILLONES A ¢700 MILLONES EN UN AÑO

Clientes bancarios indefensos ante saqueo electrónico

- Bancos alegan que clientes dan mal uso a claves de seguridad en Internet
- OIJ dice que nadie en el país puede sentirse seguro ante este tipo de delito

OTTO VARGAS M. | ovargas@nacion.com

La mañana del 11 de mayo, el abogado Luis Fernando Rodríguez encontró $4 en su cuenta del Banco Nacional en vez de los más de sus $18.000 que había ahorrado.

Tres días antes, una banda de ladrones cibernéticos transfirió –mediante Internet– el dinero a la cuenta de una vecina de Pavas y para eso utilizó su clave de seguridad personal.

MÁS SOBRE ESTE TEMA

Fondos de educadora pensionada se desaparecieron

Dinero de ingeniero pasó por cuentas

Imprimir Recomendar Disminuir Aumentar

Pese a sus reclamos, el banco no se hizo cargo de la pérdida porque "el registro transaccional reconoció su clave".

[illegible]

"Me sale que defraudaron a 10 personas. Yo no tuve ningún negocio con ellos (con los ladrones), lo tuve con el banco.

[illegible] seguro bajo mi almohada", lamentó.

Historias similares viven las más de 400 personas –242 de ellas vecinas de San José– que, de acuerdo con el Organismo de Investigación Judicial (OIJ), perdieron este año su dinero a manos de saqueadores cibernéticos.

Esa cifra supera en mucho las 120 denuncias del 2006.

Para desesperación de las víctimas, los bancos acusan el "mal uso" de las claves de seguridad para no indemnizar.

Millones virtuales. El robo virtual pareciera fuera de control. Mientras que para el 2006 las pérdidas ascendieron a ¢52 millones, para agosto del presente año el dinero sustraído ascendía a más de ¢700 millones, según estima la sección de Fraudes del OIJ.

[illegible]

[illegible]

[illegible] de los clientes, sobre los que el banco no puede asumir responsabilidad.

"Los sistemas informáticos más sofisticados y seguros, cuando reciben los datos correctos, no pueden determinar si quien los ingresa es el dueño", dijo José Francisco Araya, vocero del Banco Nacional.

La misma política aplica el Banco de Costa Rica. Ellos tampoco indemnizaron a 70 de sus clientes que reportaron saqueos entre enero y agosto de este año.

"En este caso no se vulneran los sistemas del banco, sino que el cliente se precipita en el [illegible]", dijo el subgerente [illegible].

[illegible]

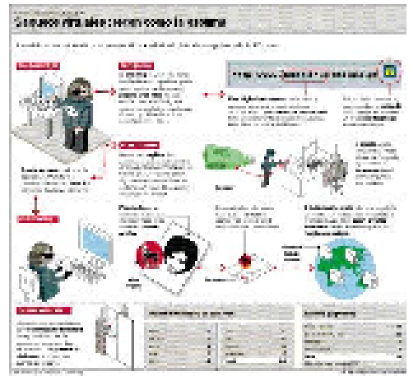
Desprotegidos. [illegible] Zapata, los clientes bancarios están atados de manos ante los robos, en especial al no existir una ley que regule el comercio electrónico.

"Hay un vacío en la legislación que deja al consumidor indefenso, pues no tiene la posibilidades técnicas o materiales de probar que fue víctima de un fraude.

"Si las entidades financieras lo colocan en esa posición, lo dejan indefenso. Debería ser responsabilidad del banco devolver al consumidor el monto y luego emprender una acción penal y civil en contra de quien realizó el fraude", dijo.

[illegible]

[illegible]



ADEMÁS EN EL PAÍS

El ICE quiere sanear el mercado

INS procura más participación en ley de mercado de seguros

[illegible]

[illegible]

Obligatorio dar aguinaldo a empleados ocasionales

6. NOTICIA: “DINERO ROBADO POR INTERNET ES RESPONSABILIDAD DE BANCOS”

Dinero robado por Internet es responsabilidad de bancos

Fuente: elpais.cr | 28/07/2009

San José, (elpais.cr) - Los bancos están obligados a responder el reintegro de dineros de los clientes, sustraídos de sus cuentas bancarias por Internet, por orden de la Sala Primera de la Corte.

Uno de los aspectos que pesó en los fallos que dictaron los magistrados de la Sala de Casación de lo Contencioso Administrativo, fue la existencia de un riesgo dentro del funcionamiento propio del servicio que las entidades financieras ofrecen en Internet.

Los magistrados consideraron que la función esencial de intermediación financiera, en dos bancos estatales, incluye la captación de fondos provenientes del ahorro del público y que lleva implícita su custodia, tanto desde el punto de vista físico como del registro electrónico.

De acuerdo con el fallo de casación, la responsabilidad que le imputó a los bancos se fundamentó en la existencia de un riesgo, como origen del daño y no en la sustracción del dinero por un tercero.

"Las pretensiones de la sociedad actora fueron acogidas por el Tribunal, quién consideró que el funcionamiento del sistema de banca electrónica presenta una peligrosidad tal que permite imputar los daños irrogados al banco", precisó una de las sentencias.

Añadió que "la experiencia confirma que las transacciones realizadas por Internet presentan cierto nivel de riesgo, por lo que las generalidades apuntadas en el considerando anterior resultan aplicables… No cabe duda que se encuentra sometida a una ineludible obligación de garantizar la seguridad de las transacciones realizadas, ya sea en ventanilla o mediante cualquier otro medio puesto a disposición de los clientes, la cual debe abarcar, necesariamente, el uso de todos aquellos mecanismos disponibles que le permitan contar con un mayor grado de certeza en cuanto a la identificación de las personas que se encuentran facultadas para

realizar transacciones electrónicas desde las cuentas", puntualizó la resolución 000394-F-S1-2009.

La Sala Primera explicó que la actividad bancaria genera por sí misma un elevado nivel de riesgo, el cual se acentúa en el servicio que se brinda por Internet , lo que demanda a la entidad un redoblamiento de los márgenes y dispositivos de seguridad en los diferentes niveles, tanto en las actividades propias y directamente desplegadas por sus funcionarios y contratistas, como en lo relativo a los medios que sus clientes deben utilizar para acceder y recibir el servicio, el cual es desplegado, promocionado e implementado por la entidad bancaria, de ahí que no puede ser admisible el argumento de la parte demandada para eximirle de responsabilidad, que Internet no es del banco.

"El medio para acceder a la plataforma del Banco no se trata, por ende, de un foco ajeno de riesgo, sino de un instrumento consustancial al servicio que presta; si se quiere, forma parte intrínseca de la actividad, que si bien es accesorio a la actividad del intermediario, resulta imprescindible", precisó la sentencia.

Explica que de allí que los mecanismos de garantía al cliente –usuario-, deben darse no solo dentro de los muros informáticos del propio Banco, sino también en el camino de acceso a él como parte del servicio.

"No en vano, el Sistema Financiero se ha abocado, en general, a la implementación de mecanismos de doble identificación, al mejoramiento de las claves y, en general, el uso de sistemas recientes como la utilización de tockens, claves cambiantes, llaves con dispositivos especiales, entre otros", puntualizó la resolución de casación de lo contencioso administrativo.

Para la Sala Primer , en aplicación del numeral 35 de la Ley del Consumidor, se apuntó la existencia de una relación de consumo dentro de la cual se produjo un daño como consecuencia de un servicio riesgoso, lo que despliega el régimen de responsabilidad objetivo, aunado al hecho de que no se demostró la existencia de causas eximentes (culpa de la víctima, hecho de tercero o fuerza mayor) que liberen de responsabilidad al Banco.

"…la responsabilidad se da por el funcionamiento del servicio, por lo que el canon de cita no tiene efectos respecto de la aplicación del numeral 35 de la Ley de Defensa del Consumidor. El fundamento de la resolución es la existencia de un riesgo que, en los términos de la Ley de Protección al Consumidor, genera el deber de reparar los daños derivados del servicio, salvo la existencia de una causal eximente de responsabilidad, lo que no implica el desconocimiento de los acuerdos –por adhesión- entre las partes", señaló la sentencia de casación.

También se resaltó la posición que debe asumir el cliente, quien tiene cumplir una serie de deberes que le impone la buena fe contractual, "…no cabe duda que es su responsabilidad el garantizar el manejo adecuado de la clave de acceso, así como seguir las recomendaciones dadas por las entidades financieras en materia de seguridad.

"La decisión de ser beneficiario de estos servicios lleva aparejado un deber de diligencia que, en caso de ser incumplido, podría liberar de responsabilidad al prestatario", apunta la resolución.

Además, indica que no resulta admisible, de acuerdo a los principios de razonabilidad y proporcionalidad, relevar al cliente de sus deberes de prudencia en aquellos aspectos que forman parte de su ámbito personal de control, como lo es el lugar donde realiza la conexión, así como utilizar equipos de cómputo adecuados y con los programas informáticos adecuados para garantizar la seguridad de la información".

Hasta el momento se registran cinco casos que la Sala Primera ha resuelto confirmar la sentencia recurrida y establece la obligación de los bancos de reintegrar a los clientes los dineros sustraídos por la Internet.

Uno de estos casos lo presentó una sociedad anónima contra el Banco de Costa Rica. El Tribunal Contencioso Administrativo y Civil de Hacienda, Sección Quinta resolvió en setiembre del 2008 declarar con lugar la demanda presentada y condenó a la entidad bancaria al pago de la suma sustraída de la cuenta corriente que ascendió a $4040, así como los intereses que se generarían a partir de la sustracción y hasta su efectivo pago. La sustracción ocurrió en enero de ese mismo año.

Esta entidad financiera también recibió una sentencia condenatoria al pago de los daños y perjuicios ocasionados contra una señora de apellido Arroyo Vargas y resarcir los fondos que le sustrajeron mediante transferencia bancaria $4379,53 en la cuenta de ahorro en dólares y ¢1 489 290 , más los intereses.

7. NOTICIA: "70 VÍCTIMAS DE FRAUDE POR INTERNET DEMANDAN A 3 BANCOS"

Costa Rica, Miércoles [illegible] de [illegible]
nacion.com /EL PAÍS

NOVEDOSA DEMANDA COLECTIVA PRESENTADA POR ASOCIACIÓN DE CONSUMIDORES

70 víctimas de fraude por Internet demandan a 3 bancos

Usuarios perdieron ¢300 millones y piden pago de daños y perjuicios a bancos Bancos Nacional y Popular rechazan alegatos; BCR estudia la demanda

[illegible] | [illegible]@nacion.com

Setenta víctimas de fraude por Internet demandaron a los bancos Nacional, de Costa Rica y Popular, mediante la novedosa figura de la demanda por intereses colectivos.

Los perjudicados perdieron, entre todos, ¢300 millones que tenían depositados en esas entidades bancarias, pues el dinero fue sustraído por terceros que ingresaron a sus cuentas.

MÁS SOBRE ESTE TEMA
Tribunal da 15 días a bancos para responder
Imprimir Recomendar
Disminuir Aumentar

Bandas organizadas utilizan diversos programas o instrumentos informáticos para robar la información de acceso a las cuentas de los usuarios. Los bancos han negado tener responsabilidad alguna en esos hechos.

Los 70 afectados piden al Tribunal Contencioso Administrativo ordenarle a los bancos el reintegro del dinero robado y el pago de daños y perjuicios.

En el país se han denunciado más de 500 casos de fraude por Internet, que ascienden a más de ¢100 millones, según el Organismo de Investigación Judicial. Ayer no fue posible obtener los datos más recientes.

La demanda fue presentada por la Asociación de Consumidores Libres (ACL), en representación de las víctimas.

Nueva normativa. La abogada de ACL, Adriana Rojas, explicó que la demanda es posible gracias al nuevo Código Procesal Contencioso Administrativo.

Dicho código da legitimación procesal a quienes invocan la defensa de intereses difusos (que afectan a todos los usuarios de la banca) o colectivos (en este caso las 70 víctimas del fraude).

Ayer, los bancos Nacional y Popular rechazaron tener cualquier tipo de responsabilidad por los fraudes.

El Banco de Costa Rica (BCR) no emitió una posición al respecto mientras analiza la demanda.

Alegatos. ACL alega que los bancos violaron los derechos de los consumidores a la seguridad, a los intereses económicos y a la información.

[illegible] empezaron a advertir a los usuarios de los riesgos que corrían con ese mecanismo.

Mientras, en el 2006 se reportaron pérdidas por ¢52 millones, en el 2007 esa cifra ascendió a ¢700 millones.

"A pesar del conocimiento de los ataques virtuales del año 2005, las entidades bancarias continuaron ocultando esta lamentable situación a sus usuarios de servicios en línea, vulnerando el derecho de información a los consumidores", indica el documento de la demanda.

La campaña de información al público se inició a finales del 2007, y ACL considera que los bancos incurrieron en "publicidad engañosa".

Los mensajes publicitarios le decían al usuario "Usarlo seguro (el servicio en línea) depende de usted", sin hacer referencia a que la banca electrónica "nunca va a ser 100% segura", sostiene ACL.

Derecho a la protección. También se alega que se violó el derecho a la protección de datos, pues los bancos [illegible] un sistema [illegible] garantizar la protección de la información bancaria de los clientes.

La Nación publicó en febrero pasado que en Costa Rica, en ese momento, muchos bancos tenían solo un mecanismo de verificación de la identidad.

En Estados Unidos, desde el 2005, las cinco autoridades financieras calificaron tal práctica como "inadecuada", y actualmente no la permiten como único medio de autenticación.

La demanda pide al Tribunal ordenar a los bancos mejorar sus sistemas informáticos y mantenerse al día con los avances tecnológicos en ese campo.

Los bancos de Costa Rica y Popular informaron que ya establecieron un paso adicional de verificación de identidad y que no se han vuelto a presentar fraudes.

Los demandantes estiman que es pertinente el pago de una indemnización porque los demandados ofrecieron un servicio sin tener las medidas de seguridad idóneas.

Al [illegible] esas vulnerabilidades del sistema se incurrió en una omisión que fue aprovechada por terceros para robar el dinero, prosigue la demanda de ACL.

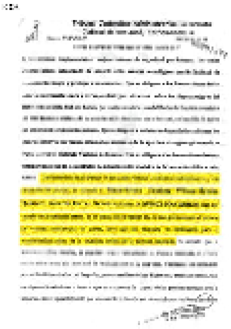
En ese sentido, se cita la responsabilidad objetiva prevista en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. De acuerdo con el artículo 35, "el productor, el proveedor y el comerciante deben responder concurrente e independientemente de la existencia de culpa, si el consumidor resulta perjudicado por razón del bien o el servicio".

Cláusulas "abusivas". Finalmente, se pide al Tribunal anular las cláusulas "abusivas" de los contratos, por ser "un abuso del Derecho".

Estas son diferentes en cada banco, pero obligan al usuario a expresar conformidad con las medidas de seguridad adoptadas por la entidad y a aceptar la responsabilidad por las consecuencias.

"Se asume al verdadero responsable por el uso fraudulento por parte de terceras personas del servicio de Internet, que la entidad bancaria ofrece al público sin protección", señala la demanda.

Tales cláusulas han servido a los bancos para rechazar los reclamos de las víctimas.



Ampliar

BANCA EN COSTA RICA

MECANISMOS INSEGUROS

La Nación publicó en febrero pasado que muchos bancos en el país utilizaban prácticas de banca en línea y proceso de los reclamos que en otros países se consideran inaceptables.
Una práctica es que, al menos en ese entonces, los bancos permitían el acceso electrónico a las cuentas bancarias con solo un mecanismo de verificación de identidad. Esa práctica en Estados Unidos se consideró inadecuada desde el 2005 y actualmente no es permitida.
Sin embargo, en Costa Rica ninguna autoridad financiera considera que le corresponde supervisar las prácticas en línea de los bancos y ninguna ley o reglamento regula los aspectos de seguridad. Ello permite a los bancos dar el servicio en los términos que desee, sin rendir cuentas a nadie, y los clientes no tienen dónde acudir, más que la Corte.
En otros países, los bancos deben reintegrar el dinero a las víctimas del fraude o probar que este ocurrió por culpa del usuario. Aquí, los bancos pueden rechazar los reclamos de los usuarios con solo suponer que el fraude de alguna forma fue provocado por ellos mismos.

alegando que los fraudes ocurren porque "el cliente ha hecho caso omiso a las advertencias del banco".

Esto pese a que en diversos casos se ha confirmado que los clientes nunca se registraron en línea, o no sabían cómo utilizar computadoras y, menos aún, Internet.

8. NOTICIA: “LAS PERSONAS SON EL ESLABÓN DÉBIL EN LA CIBERSEGURIDAD”

Las personas son el eslabón débil en la ciberseguridad: reporte

- Cantidad de páginas web con software malicioso se cuadruplicó desde principios del 2008.

Reuters
22 de julio, 2009

La popularidad de Facebook y otros muy visitados sitios de redes sociales ha dado a los "hackers" nuevas vías para robar dinero o información, dijo la compañía de seguridad Sophos en un reporte publicado el miércoles.

Cerca de la mitad de las compañías bloquea parcial o completamente el acceso a las redes sociales debido a la preocupación por ciber-incursiones a través de esos sitios, de acuerdo al estudio.

"Los resultados de las investigaciones también revelaron que un 63 por ciento de los administradores de sistemas están preocupados porque sus empleados comparten demasiada información personal a través de los sitios de redes sociales, lo que pone su infraestructura corporativa -y los datos sensibles almacenados en ella- en riesgo", dijo el reporte de Sophos.

Esto ocurre a pesar de años de exhortaciones a los usuarios de computadoras respecto a que deberían mantener su información personal en privado y abstenerse de abrir archivos adjuntos de correos electrónicos provenientes de fuentes no conocidas.

Uno de los resultados es que una cuarta parte de los negocios ha sido atacada por tácticas como el "spam", el "phishing" o ataques de software malicioso a través de Twitter u otras redes sociales, dijo Sophos.

El "phishing" es el envío de correos electrónicos a través de los cuales los estafadores tratan de convencer a sus potenciales víctimas para que revelen información personal como contraseñas o cuentas bancarias.

Sophos también descubrió que la cantidad de páginas web con software malicioso se cuadruplicó desde principios del 2008, y un 39,6 por ciento de ellas tiene sede en Estados Unidos, que alberga más que cualquier otro país. China es el segundo, con 14,7 por ciento.

Sophos, que tiene sedes en Gran Bretaña y Estados Unidos, es el mayor fabricante de software de capital privado.

9. NOTICIA: “BN Y BCR APELARON CONDENAS POR FRAUDES BANCARIOS POR INTERNET”

Costa Rica, Sábado 27 de diciembre de 2008
nacion.com /el país

SENTENCIAS ORDENAN REINTEGRAR DINERO A CLIENTES PERJUDICADOS

BN y BCR apelaron condenas por fraudes bancarios por Internet

- BN ha recibido seis condenas y BCR, dos; hay más demandas en proceso
- Ola de fraudes del 2007 se redujo con las nuevas medidas de seguridad

HAZEL FEIGENBLATT | hfeigenblatt@nacion.com

Los bancos Nacional (BN) y de Costa Rica (BCR) apelaron las sentencias que los condenaron a reintegrar el dinero a clientes víctimas de fraudes bancarios por Internet, y descartaron la posibilidad de hacer conciliación alguna.

Durante el segundo semestre de este año, al menos ocho procesos judiciales terminaron en condenas contra ambas entidades, y las responsabilizaron de las pérdidas económicas sufridas por sus clientes.

Se trató de las primeras sentencias relacionadas con la ola de fraudes electrónicos registrada en el país entre el 2007 y el 2008, y en todos los casos la decisión de los jueces se basó en el principio de responsabilidad objetiva.

Responsabilidad. De acuerdo con este, un proveedor puede ser responsable si el consumidor resulta perjudicado en razón de las características propias del bien o servicio dado, aunque no tenga la culpa.

En estos primeros juicios se determinó que terceros se apropiaron de las claves bancarias de los clientes y transfirieron el dinero a otras cuentas, de donde luego retiraron el efectivo.

Los jueces confirmaron que los sistemas de banca electrónica de esas instituciones no fueron suficientemente seguros.

Ambas entidades bancarias lanzaron sus plataformas electrónicas con solo un mecanismo de autenticación de identidad, pese a que desde el 2005 se conocía que ello era inadecuado e inseguro.

A lo largo del 2008, los dos bancos generalizaron el uso de más mecanismos de autenticación y sus representantes aseguran que no se han presentado nuevos casos.

A casación. Aunque en setiembre, tras conocer la primera condena, el BCR anunció que estaba analizando la posibilidad de no apelar, este mes el gerente, Mario Rivera, informó de que ya se plantearon los recursos de casación correspondientes a las dos sentencias recibidas.

"El Banco de Costa Rica ha continuado con el trámite de los procesos (judiciales) y en ningún caso se ha iniciado o planeado iniciar una conciliación", comentó.

El BN, que ha sido condenado en seis ocasiones, también acudió a casación.

"El Banco Nacional decidió recurrir en todos los casos a casación. En estos momentos se han presentado seis condenas en primera instancia. Cuatro ya tienen casación presentada y dos se encuentran en período de elaboración", informó la Dirección Jurídica.

Esa entidad considera que el pago o la conciliación serán procedentes solo cuando existan dos sentencias condenatorias contra el banco, ratificadas en casación.

"El problema de la conciliación radica en que somos una institución pública, y no es prudente pagar dinero (fondos públicos) sin que exista una clara certeza de que el Banco Nacional debe hacerse responsable y pagar dichos montos. Mientras el asunto no sea fallado en definitiva por las máximas instancias judiciales del país, el Banco no debe proceder a su pago", indicó la Dirección Jurídica.

Las primeras demandas presentadas por fraudes electrónicos se resolvieron en cuestión de meses debido a que el nuevo Código Procesal Contencioso Administrativo agiliza los procesos. Está por verse si la misma agilidad se dará con los casos que vayan a casación.

FOTOS

Las páginas electrónicas de los bancos costarricenses actualmente tienen más mecanismos de seguridad. Archivo

SERVICIOS SEGUROS

PROTECCIÓN AL CONSUMIDOR

El concepto de responsabilidad objetiva (un proveedor puede ser responsable si el consumidor resulta perjudicado en razón del bien o servicio, aunque no tenga la culpa) ha ido ganando terreno en el país y hoy es claro que los bienes y servicios tienen que ser seguros.
Además de las ocho recientes sentencias por fraudes electrónicos, en el 2007 los jueces lo aplicaron a favor de clientes afectados por el asalto al BN en Monteverde y a favor de un consumidor cuyo vehículo fue robado en un parqueo de Hipermás. En el 2003, se aplicó a favor de una consumidora que se resbaló en McDonald's con mayonesa derramada en el piso.

ADEMÁS EN EL PAÍS
Blandengue reglamento permite caos en colocación de vallas
Caballos, vaqueros y miles de 'águilas' participaron en el Tope
Ley de Tránsito saca a borrachos de carreteras
Temporada de huracanes estuvo intensa este año
Hoteles registran 20% menos de ocupación

En total se denunciaron más de 600 casos de fraude electrónico en todo el país y varias demandas se encuentran en proceso. Una de ellas aglutina más de 120 casos, puede incorporar a más personas y tiene demandados al BCR, BN y Banco Popular.

Más seguridad. Actualmente, la banca en línea del país opera de forma un poco más segura. La mayoría de los bancos verifica la identidad de los clientes con más de un mecanismo antes de permitir el acceso a las cuentas.

Aunque ningún sistema en línea es 100% seguro, hoy los usuarios tienen más información para protegerse de los mecanismos más comunes de robo de claves secretas, como *key loggers* (programas que se instalan en la computadora sin que el usuario lo sepa y registran todo lo que este teclea) y *phishing* (envío de correos electrónicos que parecen venir del banco y solicitan información personal).

Además, con el uso de segundos mecanismos de autenticación las claves ya no son suficientes para tener acceso a las cuentas, pues también se requiere un código diferente cada vez que se hace la conexión. El delincuente tendría que robar físicamente el dispositivo que contiene tales códigos.

Por su parte, el Organismo de Investigación Judicial ha desarticulado varias bandas dedicadas a cometer este tipo de delito.