UNIVERSIDAD DE ORIENTE
NÚCLEO DE SUCRE
ESCUELA DE ADMINISTRACIÓN
DEPARTAMENTO DE ADMINISTRACIÓN

Delitos Cometidos en los Cajeros Automáticos y su Impacto en los Usuarios y la Institución Financiera (Banesco) Sucursal de Cumaná, Estado Sucre. Durante el Periodo 2007-2008.

Autores:
Br: Ortiz S. David J
Br: Ortiz A. José R

Trabajo Final de Curso Especial de Grado Presentado Como Requisito Parcial Para Optar al Título de Licenciatura en Contaduría Pública

Cumaná, abril de 2008

UNIVERSIDAD DE ORIENTE
NÚCLEO DE SUCRE
ESCUELA DE ADMINISTRACIÓN
DEPARTAMENTO DE ADMINISTRACIÓN

DELITOS COMETIDOS EN LOS CAJEROS AUTOMÁTICOS Y SU IMPACTO EN LOS USUARIOS Y LA INSTITUCIÓN FINANCIERA (BANESCO) SUCURSAL DE CUMANÁ, ESTADO SUCRE. DURANTE EL PERIODO 2007-2008.

Autores:
Br: Ortiz S. David J
Br: Ortiz A. José R

ACTA DE APROBACIÓN DEL JURADO

Trabajo de Grado APROBADO en nombre de La Universidad de Oriente, por el siguiente jurado calificador, en la ciudad de Cumaná, a los 16 días del mes de Abril de 2008.

_____

Prof. Rafael García

Facilitador

C.I.: 10.462.247

INDICE

DEDICATORIA

Ante todo, a mis protectores y guías espirituales “Dios Todo Poderoso y la Virgen del Valle”, a los cuales siempre pido por la protección del mundo y a todos mis seres queridos, en especial a mi familia y mi novia.

A mis padres Reinaldo y Nelly, por todo el amor, consejos y apoyo incondicional, lo cual me encaminó a lograr todas mis metas y en especial la de culminar mi carrera universitaria.

A mis hermanas, Victoria y Virginia, a las que amo y adoro con todo mi corazón, y que este logro y triunfo en mi vida les sirva de ejemplo para que no decaigan en todas las aspiraciones que se propongan.

A mi novia Yesenia, ya que con su alegría, humildad y perseverancia, me inspiró para superar todos los obstáculos que se me presentaron en mi vida personal y como estudiante.

A todos mis compañeros de estudios, que siempre compartieron conmigo momentos de alegría y tristezas, y en especial a Charlys Cedeño, quien con su lucha diaria, siempre buscó la unión entre todos los estudiantes. “Hermano tu Amistad y tus Recuerdos quedarán siempre entre nosotros”.

Ortiz S. David J.

DEDICATORIA

Primeramente a Dios y al Divino Niño, por darme salud, vida y fortaleza para seguir adelante y poder alcanzar mis sueños, Bendito seas mi Dios.

Con mucho cariño principalmente a mi Mamá Luisa Carmen Arcia, por todo su apoyo, confianza, dedicación, sacrificios y esfuerzo para sacarme adelante, de verdad no tengo como pagarte todo lo me has dado, Te Amo Mamá, Gracias por ser más que mi madre, mi amiga, y fiel compañera, Dios te Cuide y te Bendiga Hoy, Mañana y Siempre.

A Cruz Rengel por todo su apoyo, cariño, comprensión y confianza, y aunque no corre su sangre por mis venas lo quiero como si fuera mi Padre, no te imaginas cuanto Te Quiero, Gracias por todo, hoy afirmo esa frase que reza, Padre no es el engendra sino el que Cría y para mi tu eres mi padre gracias por el ejemplo que me has dado, Dios te Bendiga y te de Muchos años de vida, te estaré agradecido toda la vida.

A mi Abuela Rafaela Arcia, que aunque no esta conmigo físicamente se que donde quiera que este me esta mirando y dándome su bendición, Te Quiero abuela nunca te olvidare vivirás por siempre en mis recuerdos y en mi corazón.

Ortiz Arcia José R.

AGRADECIMIENTO

A los profesores Carmen Rosa Silva, Danny Delgado y Rafael García, por facilitar todas las herramientas necesarias para el desarrollo de la investigación.

A la gerente de la Entidad Financiera BANESCO, Lic. María Gómez, por suministrar la información necesaria para la elaboración de la investigación.

A todos mis compañeros del Curso Especial de Grado de Economía Digital, por todos los consejos, ayuda y amistad que me proporcionaron para la confección del Trabajo de Grado.

A mi compañero José Ortiz, por aportar todo su conocimiento y empeño en la elaboración de la investigación.

Ortiz S. David J.

AGRADECIMIENTO

A todos mis profesores y profesoras que en todos estos años me enseñaron más que números y letras, en especial al Profesor Rafael García gracias por su ayuda, apoyo y colaboración, a Carmen Rosa Silva, Danny Delgado, Juan C Mota, gracias por su contribución en la realización de este trabajo.

A la Lic: Maria Gómez, Gerente del Banco Banesco, gracias por su tiempo, apoyo y colaboración, en la elaboración de este trabajo.

A Maria Elena (mi Nena) gracias por estar conmigo y apoyarme siempre, gracias por todos los buenos momentos que hemos compartido juntos, Te Quiero eres Súper Especial, Tefi Afimofi Mufichofi.

A todos mis compañeros del Curso Especial de Grado de Economía Digital, muchas gracias por su amistad, apoyo, y por todos los buenos momentos que compartimos en este tiempo.

A Carmen, Arianny, Johana, Diamaris, Carolina, David, Yesenia, Antonio, Humberto, y a todas las personas que me apoyaron siempre de manera incondicional muchas gracias, a Yosanny, Javier, Ezequiel, Nelson, de verdad gracias a todos por su apoyo y por los buenos momentos que compartimos juntos que Dios los Bendiga a todos Hoy, Mañana y Siempre.

Ortiz Arcia José R.

LISTA DE TABLA

RESUMEN

El desarrollo del Comercio Electrónico constituye un instrumento cuyo crecimiento es impresionante, en la actualidad el sector bancario ha implementado el uso de la tecnología para garantizar que sus usuarios realicen las operaciones de manera efectiva a través del uso de los llamados cajeros automáticos. El constante crecimiento de la tecnología ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con animo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales, tanto en la sociedad como en las Instituciones Financieras. Pero la cuantía de los perjuicios ocasionados por los Delincuentes Informáticos es a menudo superior a la que usualmente comete la delincuencia tradicional, y también son mucho más elevadas las posibilidades que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces, muchas veces de borrar toda huella de los hechos cometidos. En este sentido, la información puede ser el objeto del ataque o el medio para cometer otros Delitos en los Cajeros Automáticos.

INTRODUCCIÓN

La tecnología en las últimas décadas ha permitido cambios en nuestro modo de vida, pasando de lo convencional a lo innovador, provocando la generación de nuevos avances tecnológicos e incrementando la evolución de la sociedad en todos los ámbitos (comercial, profesional, informativo, formas de comunicación, entre otros). La transformación que ha sufrido la sociedad ha dado paso a grandes oportunidades en las empresas a través de las comunicaciones, destacando que éstas reducen sus gastos por el uso de la tecnología que se encuentran a la disposición de grandes, medianas y pequeñas empresas. El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez más y creando nuevas formas de comercio, en las entidades financieras ha generado un alto grado de competitividad entre ellas, innovando constantemente sus tecnologías para mayor beneficio, comodidad y mantenimiento en el tiempo de los usuarios en los bancos, en este marco se desarrolla la Banca Electrónica.

Para optimizar aún más el trabajo y prestar un mejor servicio a los usuarios por la creciente demanda de clientes para resguardar sus ahorros o patrimonios, muchas instituciones financieras han cambiado sus mecanismos adaptándolos a las nuevas tecnologías, es por ello que implementaron un sistema que les permitiría agilizar las transacciones realizadas en las instituciones financieras y para ello se diseñaron los cajeros automáticos.

Éstos equipos proporcionan grandes ventajas en cuanto a las nuevas tecnologías de la información, como una nueva forma de inmediatez, para la obtención de dinero en efectivo las 24 horas del día durante todo el año, con la particularidad de que se pueden realizar una serie de operaciones como por ejemplo (retiros de efectivo, consultas de saldo, transferencias entre cuentas, cambios de claves, entre otros), y poder efectuar transacciones financieras con mayor rapidez y seguridad brindando mayor comodidad al cliente, siendo éste un equipo electrónico mediante el cual el cliente tiene la oportunidad de realizar diferentes operaciones financieras a través del uso de una tarjeta de débito o crédito activadas por claves secretas personales que permiten conectar al cliente con el computador central del banco.

En la actualidad muchos bancos han optado por instalar para bienestar de sus clientes un mayor número de cajeros automáticos, implementando nuevas tecnologías para que puedan así realizar sus

operaciones con la mayor seguridad posible, a pesar de todas las formas de seguridad que hay para el uso de los cajeros automáticos, estas transacciones tienen un alto porcentaje de riesgo, fraude o alteración de datos personales, muchas de las actualizaciones que realizan los bancos por lo general no son conocidas por los usuarios de manera oportuna, ocasionando incomodidad, requerir mayor tiempo para realizar operaciones y solicitar ayudas de terceros haciéndolos más vulnerables de ser objetos de manipulación y ser así victimas de robos por medio de la creatividad delictiva en el área de la informática que ha impuesto su poder incontrolable, perjudicando a los usuarios y entidades bancarias por medio de los delitos electrónicos a los sistemas de los cajeros automáticos.

Esta situación genera un daño financiero en el patrimonio de los usuarios y los bancos, que en su mayoría se sienten impotentes ante los fraudes electrónicos tan frecuentes en los sistemas, debido a esos menoscabos no han permitido el éxito de los cajeros automáticos en la actualidad, pero se aspira superar estos obstáculos que han impedido su normal proceso de desarrollo, para que de esta manera se convierta en una equipo confiable para efectuar operaciones con la mayor seguridad posible.

Muchas de las instituciones financieras han optado por implementar de manera forzosa medidas de seguridad en sus cajeros automáticos como consecuencia de la creciente ola de delitos que se han venido suscitando en ellos, muchos ocasionados por el acelerado crecimiento de las tecnologías delictivas, otros por los analfabetas tecnológicos y su mal uso de los cajeros, poco conocimiento por parte de los usuarios de los delitos que se están cometiendo en su mecanismo de rápida transacción, faltas de los bancos por la no información de sus usuarios de las medidas de seguridad implementadas por ellos.

Las innovaciones en materia de medidas de seguridad dan lugar a la modificación en la información, la toma de decisiones y el proceso de organización y planificación del trabajo dentro de las instituciones financieras, al punto de que éstas sean mejores proveedoras de servicios a sus usuarios, creciendo a un ritmo acelerado en términos de calidad y confiabilidad. Los principales desafíos en los que se encuentran las entidades financieras podrían resumirse en la necesidad de tener una mayor eficiencia, rentabilidad, fortalecimiento y el manejo oportuno del recurso humano y tecnológico.

CAPÍTULO I:
EL PROBLEMA

1.1 Planteamiento Del Problema.

El auge del comercio electrónico constituye un instrumento cuyo crecimiento es impresionante, en la actualidad el sector bancario ha implementado el uso de la tecnología para garantizar que sus usuarios realicen las operaciones de manera efectiva a través del uso de los llamados cajeros automáticos, gracias a estos no es necesario portar dinero en efectivo, solo basta la utilización de una tarjeta inteligente en la cual tendremos nuestros créditos y a través de la cual podemos cancelar el transporte publico, cines, parques, etc. Son innumerables los productos y servicios que se pueden adquirir y cancelar a través de las tarjetas de crédito o debito. Sin embargo, junto a las incuestionables ventajas que estas nos ofrecen comienzan a surgir algunas facetas negativas, como por ejemplo, lo que se conoce hoy día como criminalidad informática.

El desarrollo de la tecnología ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con animo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales tanto en la sociedad como en las instituciones financieras.

Pero la cuantía de los perjuicios ocasionados por los delincuentes informáticos es superior a la que usualmente comete la delincuencia tradicional, y también son mucho más elevadas las posibilidades que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces, muchas veces de borrar toda huella de los hechos cometidos. En este sentido, la información puede ser el objeto del ataque o el medio para cometer otros delitos en los cajeros automáticos.

Venezuela es uno de los tantos países, donde se ha venido incrementando los delitos electrónicos a través de los cajeros automáticos, los diferentes fraudes cometidos van en detrimento de quienes operan comercialmente a través de este medio. Según Trino Alcides Díaz, en los últimos años, se ha venido

estudiando el fenómeno de los fraudes electrónicos y se ha determinado que existen varios tipos de delitos o fraudes que se cometen y se repiten cotidianamente en nuestro país, como es la duplicación o clonación de tarjetas, que se basa en la utilización de una maquina pescadora que copia la información de la banda magnética que tiene la tarjeta de crédito o debito, también se encuentra el Phishing, el cual se trata de la utilización de correos electrónicos por personas que se hacen pasar por una empresa de confianza para obtener datos bancarios confidenciales de forma fraudulenta, por otra parte se encuentra el Phishing telefónico, en esta modalidad los delincuentes realizan llamadas telefónicas haciéndose pasar como representantes de una organización especialmente instituciones bancarias, en donde los clientes son persuadidos a llamar a una línea telefónica directa, y de esta manera obtener información de cuentas y datos confidenciales por medio del engaño, como podemos observar son innumerables los delitos electrónicos de los cuales pueden son victimas los venezolanos.

Así mismo, Roberto León Parilli señaló que en menos de tres semanas la asociación que preside recibió 10.000 denuncias por clonaciones de tarjetas y relata que cinco de cada diez venezolanos son victimas de este crimen. Por otra parte indicó que para el mes de octubre de 2007 habían recibido 57.500 denuncias de los cuales han sido procesadas 5.182 por clonación de tarjetas de crédito y cobro de intereses sobre intereses, y las mismas fueron consignadas ante la Superintendencia de Bancos y Otras Instituciones Financieras para su debido estudio y pronunciamiento, ya que los respectivos bancos en forma unilateral han declarado improcedentes los reclamos, además de solicitar la revisión inmediata de las líneas de crédito para determinar si se ha incurrido en el cobro de intereses sobre intereses, en cuyo caso requerirían la devolución de las cantidades indebidamente cobradas.

En el país el número de denuncias sobre estafas a tarjeta habientes que les han sustraído dinero de sus cuentas aumenta todos los años, según José Ángel Rivero, presidente de la Comisión de Servicios Bancarios y Financieros del Indecu. Aunque no ofreció datos de otros años, aseguró que durante el 2007 han recibido 10.000 casos de personas víctimas de irregularidades en sus tarjetas. En promedio, están procesando 1.250 expedientes mensuales y estiman que si continúan con este ritmo de reclamos podría desbordarse la capacidad que tienen para atender a los ciudadanos en materia bancaria.

De esos 10.000 expedientes el 70% se corresponde a ilícitos que han sufrido los usuarios en los cajeros automáticos. El 30% restante son clonaciones, tanto a tarjetas de débito como de crédito. En

pérdidas económicas al sumar los montos de cada una de las denuncias se obtienen millardos de bolívares, señaló Rivero.

La directora de la Oficina Municipal de Protección al Usuario de Puerto La Cruz (Omdecu), Alicia Silvia, aseguró que en su jurisdicción durante 2007 reportaron 589 casos de este tipo, de los cuales sólo 40% ha tenido respuesta por parte de las empresas del ramo.

Lo antes mencionado, es una muestra de alguna de las cifras que indican el grado de impunidad reinante en materia de delitos electrónicos, lo cual a medida que transcurre el tiempo se ha incrementado y que perjudica sensiblemente el sano intercambio y desenvolvimiento de las transacciones electrónicas efectuadas por quienes si quieren hacer las cosas de manera productiva y de quienes actúan de buena fe.

Por otra parte, cabe destacar que efectivos de inteligencia del (CICPC) a nivel nacional, indicaron que las bandas de los llamados "tarjeteros" operan con mayor frecuencia en los estados Nueva Esparta, Anzoátegui y Bolívar, así como también en los hoteles cinco estrellas de las grandes ciudades. La razón es que en esos lugares es más probable encontrar a usuarios de cajeros automáticos que posean tarjetas internacionales.

De igual manera, la incidencia de la criminalidad informática a través de los cajeros automáticos se ha hecho sentir en gran parte de los estados que conforman el territorio nacional, el Estado Sucre es uno de los estados donde se a incrementado la criminalidad informática, según reporte de la Comisión integrada por la brigada turística, división de inteligencia y motorizados de la policía, durante los meses de octubre y noviembre de 2007 se detuvieron 25 personas procedentes de diferentes Municipios del Estado los cuales están involucrados con la clonación de tarjetas de crédito.

Los daños, perjuicios, desilusiones y otras consecuencias que puede generar los hechos que representan los engaños producidos producto bien sea, por la ingenuidad o por la falta de información acerca del manejo de los cajeros y el uso de las tarjetas lo que podríamos definirse como Analfabetismo Electrónico producto de la incapacidad de manejar las nuevas tecnologías por falta de conocimiento, ignorancia o exclusión, lo cual hace a los usuarios más vulnerables de ser victimas de fraudes electrónicos que pueden ser cuantificables y ruinosos para quienes sean fraudados.

Las instituciones financieras y usuarios de la ciudad de Cumaná no se escapan de ser objeto de este tipo de delitos, ya que el grado delictivo se ha incrementado considerablemente en lo que a materia de criminalidad informática se refiriere, según el Comisario de la Policía Científica **(**CICPC) Jesús Castillo, en la cuidad de Cumaná, ocurren lo que se conoce como el "cambiazo", indico Castillo que durante los últimos dos meses ya se han imputados 12 personas y aun se investiga a otras 80 personas más que pudieron participar este tipo de estafa.

Es por ello que hoy día los usuarios o personas deben conocer y obtener información acerca del manejo de los cajeros automáticos y adaptarse a los cambios tecnológicos que estos puedan presentar en el futuro, puesto que este sistema computarizado con el que se maneja la recepción y entrega de efectivo, así como los diferentes servicios que ofrece la instituciones bancaria, no están exentos de manipulación que puedan ir contra la seguridad bancaria y de sus usuarios.

En tal sentido y producto del planteamiento antes mencionado surge la necesidad de plantear las siguientes interrogantes:

¿Cuál es el impacto de los delitos cometidos en los cajeros automáticos para los usuarios e instituciones financieras?

¿Qué tipos de delitos informáticos son cometidos en los cajeros automáticos de las instituciones financieras objeto de estudio?

¿Qué medidas de seguridad han implementado las instituciones financieras para evitar este tipo de delitos?

¿Señalar el funcionamiento de los mecanismos de seguridad de los cajeros automáticos?

¿Cuál es el marco jurídico que regula los delitos informáticos?

¿Qué acciones han implementado SUDEBAN para la protección de los usuarios e instituciones financieras?

1.2. Objetivos

1.2.1 General

Analizar los delitos cometidos en los cajeros automáticos y su impacto en los usuarios y la institución financiera (Banesco), Avenida Bermúdez, sucursal de Cumaná, estado sucre. Durante el periodo 2007-2008.

1.2.2 Específicos

Analizar el impacto de los delitos cometidos en los cajeros automáticos para los usuarios e institución financiera.

Describir que tipo de delitos informáticos son cometidos en los cajeros automáticos de la institución financiera objeto de estudio.

Señalar las medidas de seguridad que han implementado la institución financiera para evitar este tipo de delitos.

Describir el marco jurídico que regula a los delitos informáticos.

Señalar las acciones implementadas por SUDEBAN para la protección de usuarios e instituciones financieras.

1.3 Justificación

El auge e impacto que ha generado la clonación de tarjetas de débitos y créditos, a través del uso de los cajeros automáticos extendidos en el ámbito nacional por las diferentes entidades financieras, ha causado un malestar general en la sociedad venezolana que hacen uso a diario de estos dispositivos electrónicos, con el fin de facilitar los mecanismos de disponibilidades de dinero en efectivo. Esta problemática ha generado un impacto psicológico negativo en la población que la ha llevado a disminuir el uso y confianza de esta tecnología.

La escasa información existente por parte de las instituciones financieras hacia los usuarios y

personas que deseen indagar sobre el uso y funcionamiento de estos equipos electrónicos, nos ha llevado a desarrollar esta investigación, que a su vez, permitirá suministrar información oportuna a los usuarios a cerca de los diferentes delitos o fraudes que se vienen cometiendo en muchos cajeros automáticos, y conocer las diferentes medidas de seguridad implementadas por los bancos en cuanto a estos delitos. Las entidades financieras se beneficiarían por el grado de credibilidad por parte de los usuarios e incrementarían los ingresos obtenidos a través de las comisiones por la ejecución de operaciones en los cajeros automáticos, puesto que los clientes se encontrarían debidamente informados; tomando de esta manera sus previsiones al momento de realizar las operaciones.

En tal sentido, se proporcionará a los usuarios, las herramientas necesarias al momento de hacer uso de un cajero automático y no ser victimas de robos o fraudes. Asimismo, se les facilitará los pasos que deben seguir para formular la denuncia al banco en caso de ser objeto de un fraude electrónico.

1.4 Metodología

Para toda investigación es fundamental que los resultados obtenidos o nuevos conocimientos tengan el máximo grado de exactitud y confiabilidad, para ello se plantea una metodología o procedimiento ordenado que se sigue para establecer lo significativo de los hechos y fenómenos hacia los cuales esta encaminado el interés de la investigación.

Por lo anteriormente expuesto, en este capitulo se indica el tipo y nivel de la investigación, se identifica la población. Además de ello, se especifican las fuentes de información y las estrategias de recolección de datos de la misma.

1.5 Tipo De Investigación

El tipo de investigación que se llevará a cabo en el presente trabajo es documental y de campo. En tal sentido Ramírez (1999), plantea que: “Se le llama también investigación sobre el terreno. Es importante realizar este tipo de investigaciones ya que, siendo su objeto natural de estudio el hombre y sus acciones, es perfectamente pertinente abocarse a estudiar estos fenómenos en la realidad misma donde se producen.” (P.77).

Por otro lado Arias, F. (2006), establece lo siguiente: “La investigación documental, es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas”. (P.27).

Las definiciones planteadas con anterioridad, guardan estrecha relación con la investigación que se realizará, por tal motivo, se evaluará los delitos cometidos en la institución financiera en estudio, esto indica que será indispensable dirigirse al lugar donde se dan los hechos y así recolectar los datos primarios para la realización de la investigación, a su vez, indagar en datos secundarios para desarrollar el proyecto.

1.6 Nivel De La Investigación

El nivel de la investigación será descriptivo. Al respecto Sabino, C. (2002), señala que: “Las investigaciones descriptivas utilizan criterios sistemáticos que permiten poner de manifiesto la estructura o el comportamiento de los fenómenos en estudio, proporcionando de este modo información sistemática y comparable con la de otras fuentes”. (P.43).

La investigación que se llevará a cabo tiene un nivel descriptivo, debido a que se indagará en la incidencia de los delitos cometidos en los cajeros automáticos de la institución financiera y sus usuarios, así como también describir las medidas de seguridad que vienen implementando la entidad financiera para evitar este tipo de delitos.

1.7 Área De Estudio

EL área de estudio seleccionada para esta investigación será la institución financiera (Banesco), dicha institución se encuentra ubicada específicamente en la Avenida Bermúdez de la ciudad de Cumaná, Estado Sucre.

1.8 Población

La población en estudio estará compuesta por 2 empleados de la institución, siendo estos los sujetos en estudio para la presente investigación.

La población es definida según Arias, F. (1999) como el "conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Ésta queda delimitada por el problema y por los objetivos del estudio" (P.81).

1.9 Alcance Y Limitaciones

Alcance

Esta investigación sólo tomará en cuenta el estudio y análisis de los Delito Informático en la Institución Financiera BANESCO, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega La Banca Electrónica ante éste tipo de hechos.

Limitaciones

La principal limitante para realizar ésta investigación, estuvo enmarcada por la poca información sobre las estadísticas de denuncias realizadas por parte de los usuarios en las entidades financieras, las cuales no aportaron la información necesaria para este trabajo, según representantes de este sector, esa información se considera confidencial, lo cual si tomamos en cuenta el punto de vista de la instituciones es razonable, porque todo el prestigio y la confianza que depositan los clientes en los bancos se basa en la seguridad que este le brindan de garantizar el resguardo de su dinero, por tal razón existe temor por parte de los bancos de que esas estadísticas sean dadas a conocer, ya que muchas de esas denuncias no proceden o no son aprobadas por el banco, lo que origina que el cliente pierda su dinero ocasionando un daño al capital personal de los usuarios.

Por su parte el CICPC de la delegación de Cumaná a pesar que cuenta con un departamento de Delitos Informáticos, éste no pudo suministrar información referente al desarrollo de la investigación ya que esta división es prácticamente nueva y los datos estadísticos sobre la denuncia de delitos informáticos en cajeros automáticos es escasa por cuanto los usuarios no denuncian la irregularidad a

esta institución sino que lo hacen directamente al banco.

1.10 Técnicas E Instrumentos De Recolección De Datos

De acuerdo con Arias, F. (2006) “las técnicas de recolección de datos es el procedimiento o forma particular de obtener datos o información” (P.67). Son ejemplos de técnicas: la observación directa, la encuesta en sus dos modalidades (entrevistas o cuestionarios), el análisis documental, análisis de contenido, entre otros. Así mismo, Arias define los instrumentos de recolección de datos como, “los medios materiales que se emplean para recoger y almacenar la información” (P.69). Ejemplos: fichas, formatos de cuestionarios, guías de entrevistas, lista de cotejos, grabadores, entre otros.

A fin de recabar la información de la siguiente investigación, la técnica de recolección de datos utilizada fue la entrevista semi-estructurada, la cual es definida por Arias, F. (2006) “Aun cuando existe una guía de preguntas, el entrevistador puede realizar otras no contempladas inicialmente. Esto se debe a que una respuesta puede dar origen a una pregunta adicional o extraordinaria” (P.74).

1.11 Fuentes De Información

Las fuentes de información pueden tener origen primario y secundario. Para efectos de esta investigación las fuentes primarias están dadas por la información recolectada a través de las entrevistas aplicadas directamente a los representantes de la entidad financiera (Banesco). Por otro lado, la información secundaria está constituida por las bibliografías especializadas (tesis, trabajos de ascenso), artículos de periódicos, internet, observación directa.

CAPÍTULO II:
CAJEROS AUTOMÁTICOS

2.1antecedentes De La Investigación

Con el fin de indagar acerca de investigaciones que se han realizado en el área de la banca electrónica y su incidencia en la prestación de servicios financieros se halló un trabajo titulado: "Análisis de los Aspectos Negativos del Dinero Electrónico en las Transacciones Bancarias Venezolanas", presentado por Br. Aguado, A. y Luna, Y. (2007), dentro de las principales conclusiones señalan que:

"Los cajeros automáticos proporcionan rapidez y comodidad para realizar transacciones financieras, sin embargo no se descarta la posibilidad de que la información que se utiliza para la operatividad de los mismos por parte de la banca y los usuarios sea interceptada por terceras personas dedicadas a cometer fraudes electrónicos para su beneficio en detrimento de los usuarios y la banca".

Por otra parte se consultó con los antecedentes de un trabajo de investigación realizado por los Br. Cordero, V. y Sifonte, S. (2007). Titulado: "Banca Electrónica Una Herramienta para el Desarrollo de Ventajas Competitivas". Dentro de sus principales conclusiones se encuentra que:

"Las debilidades presentadas por los servicios de banca electrónica son falta de información en temas relacionados con las alianzas estratégicas y seguridad de los usuarios"

2.2. Bases Teóricas

2.2.1 Historia De Banesco

Venezuela otorga la calificación nacional bancaria de corto plazo F-3 (ven) y la calificación nacional bancaria de largo plazo BBB (ven) a Banesco Banco Universal C.A. (BANESCO). Dichas calificaciones se encuentran soportadas por su amplia participación de mercado que le ha permitido mantener una adecuada diversificación de operaciones y exposiciones crediticias, todo esto junto al

potencial de negocios derivados de la incorporación de las diferentes clientelas de las instituciones fusionadas. Por su parte, la calificación se encuentra limitada por una relativa mayor morosidad y el efecto de las plusvalías sobre el patrimonio. Adicionalmente y común al resto del sistema, la institución debe enfrentarse a las presiones impuestas por un nivel de competencia creciente, los efectos de un ambiente macroeconómico inestable y el incremento de la intervención gubernamental en el negocio bancario. Las calificaciones BBB (ven) denotan una buena calidad crediticia e indican que actualmente hay una baja expectativa de riesgo de crédito. La capacidad de pago oportuno para con los compromisos financieros es considerada adecuada, pero cambios adversos en la marcha del negocio o en las condiciones económicas podrían afectar dicha capacidad.

Durante el período 1992 hasta 1997 y al igual que muchos de los grupos financieros presentes a la fecha, la institución operaba a través de diferentes entidades financieras que cubrían todos los segmentos de la actividad bancaria a nivel nacional, siendo que durante el segundo semestre del año 1997 las autoridades autorizaron su conversión a Banco Universal, mediante la fusión de algunas de las entidades financieras especializadas que conformaban el llamado “Grupo Financiero Banesco” (empresa de arrendamiento financiero y fondo de activos líquidos). A partir del año 1996 también se inició la formación de una de las mayores entidades de ahorro y préstamo en Venezuela, la cual se formó en el año 1999 mediante la fusión de 7 entidades de ahorro y préstamo regionales, siendo que la entidad resultante (Caja Familia Entidad de Ahorro y Préstamo - CF) mostraba una estructura accionaria similar a la de BANESCO. Al momento de su creación CF era una de las instituciones líderes en el segmento de financiamiento hipotecario.

Durante el año 2001, Caja Familia se fusionó con Banco Unión C.A. (BU), uno de los mayores bancos comerciales en dicha fecha, el cual se caracterizaba por un claro liderazgo en el segmento de personas y dentro del negocio de tarjetas de crédito. Esta fusión resultó en la creación de Unibanca Banco Universal (UNIBANCA), el cuarto mayor banco del país al momento de su creación. Posteriormente, en el año 2002, BANESCO se fusionó con UNIBANCA y otras instituciones financieras especializadas del denominado “Grupo Unión”, lo cual le permitió reducir la diferencia de tamaño entre BANESCO y el tercer banco más grande del país en ese momento. Dicho programa de fusiones y adquisiciones no sólo requirieron de un agresivo plan de inversión en tecnología, sino también del cierre de numerosas agencias bancarias que se solapaban, la racionalización de la plantilla

laboral y, por último, un agresivo programa de mercadeo para reafirmar la solidez de la marca. Tales gastos han resultado en una significativa plusvalía la cual deberá ser amortizada en un período de 20 años, lo cual reduce la calidad del patrimonio de la institución. Al cierre de diciembre de 2002 dichas plusvalías alcanzaban el 23% del patrimonio, de los cuales 18% corresponden a la fusión con UNIBANCA, mientras que el restante 5% corresponde a otras fusiones de menor cuantía realizadas en años anteriores.

Durante el primer trimestre del año 2003, BANESCO ha mantenido una estrategia proactiva para mantener e incrementar su posición de mercado, principalmente a través de una agresiva captación de depósitos en todos los segmentos del mercado. Al cierre de marzo de 2003, la relación de morosidad ajustada se redujo ligeramente hasta 8,9%, principalmente gracias al mantenimiento de la cartera de créditos bruta y la aplicación de algunos castigos de cartera, dicha relación se compara favorablemente con el promedio del mercado (11%). Por su parte, la reducción de las provisiones de cartera producto de los castigos de préstamos realizados, se reflejó en una reducción de la relación de cobertura ajustada de cartera morosa, la cual se ubicó en 160%, aún muy por encima del promedio del mercado.

2.2.2 Misión

Es una Organización de servicios financieros integrales, dedicada a conocer las necesidades de nuestros clientes, y satisfacerles a través de relaciones basadas en confianza mutua, facilidad de acceso y excelencia en calidad de servicio.

Dentro de su ramo es líder en los sectores de Persona y Comercio, combinando tradición e innovación, con el mejor talento humano y avanzada tecnología.

Se encuentra comprometido a generar la mayor rentabilidad al accionista y bienestar a nuestra comunidad

2.2.3 Valores

Integridad y Confiabilidad.

Defender la confidencialidad de nuestros clientes, manejando honestamente nuestros negocios, actuando de manera congruente entre lo que somos, decimos y hacemos.

Responsabilidad Individual y Social.

El éxito de la organización se basa en que cada persona Banesco responde por el impacto de sus acciones en su hogar, la empresa y la sociedad.

Innovación y Calidad de Servicio.

Esta dispuestos a romper con paradigmas para superar permanentemente las expectativas de nuestros clientes.

Emprendimiento.

Fomentar el pensamiento y acción del trabajador como dueño del negocio para asegurar el éxito propio y de la empresa.

Interdependencia y Liderazgo.

Promover el liderazgo justo e inspirador, capaz de desarrollar alianzas, potenciar talentos y construir equipos exitosos en beneficio de la organización.

Renovación y Excelencia Personal.

Impulsar el crecimiento integral de todos y cada uno de los miembros de la organización para permanecer en la vanguardia del conocimiento y su aplicación en el negocio.

Diversidad y Adaptabilidad.

Fomentar la capacidad de adaptación a nuevas realidades, mercados y culturas en la ejecución de nuestros negocios.

2.3 Origen De Los Cajeros Automáticos

Según Stav, Julie. (2007). SHEPERD-BARRON, fue el creador del cajero automático, al modificar una maquina que en vez de dispensar chocolates, dispensara dinero, todo esto surgió, cuando él se dirigía al banco Barclays de Londres y por llegar unos minutos tardes no pudo retirar su dinero. De inmediato empezó a trabajar en su proyecto y dos (2) años más tarde, el 27 de junio de 1967, se inauguro el primer cajero automático frente a una sucursal del banco Barclays, en la localidad de Enfield, al norte de Londres.

El primer cajero automático instalado en la sucursal de Barclays, utilizado para su funcionamiento cheques radioactivos estampados con una pequeña cantidad de carbono.

González, E. (S/F), establece que la Banca Venezolana como en todos los países del mundo ha ido evolucionando hacia un negocio de prestación de múltiples servicios, dentro de los cuales los no financieros están ganando terreno de forma rápida y significativa.

La prestación de servicios de sistemas de pagos, entre otros, no considerados tradicionalmente como servicio financieros, desde hace ya algunos años representa una fuente importante de negocios y de rentabilización de la actividad bancaria en general. En Venezuela como en otros países del Mundo la reducción que ha experimentado los índices de intermediación financiera, han obligado a la Banca a rentabilizar sus negocios por medio de la prestación de otros servicios.

Es de esta manera, que la banca personalizada y los servicios que por medio de esta podrían ofrecerse a los clientes, empezó a cobrar relevancia. Los cajeros automáticos o ATM¨S (Automatic Teller Machina), empezaron entonces entrados los años 80, a constituir un atractivo de ahorro de tiempo para los clientes bancarios y posteriormente una fuente de ahorro de costos para la gestión bancaria.

Con el fin de concretar la interconexión entre las redes y cajeros operativos en el mercado hasta la

fecha, un grupo de bancos entre los que se encontraban, Provincial, Venezuela, Caracas y Venezolano de Crédito, iniciaron sus conversaciones.

El 31 de agosto de 1987, se resalta como hito en la historia de los cajeros automáticos en Venezuela. En esta fecha se constituye la Corporación SUICHE 7B, C.A, como la empresa de servicio de interconexión, bajo el lema: “Su ingreso cómodo hacia la electrobanca: 7 días completos de banca a la semana”. La propia corporación reconoce que este año transcurrió saturado de investigaciones, pruebas y ensayos.

Se ha reconocido que la iniciación de las operaciones y servicios prestados por medio de los cajeros automáticos no fue fácil. La corporación reseña que para agosto de 1988, la Red se encontraba constituida por tan solo 50 cajeros. Más adelante en la década de los 90 fue motivado por el mejoramiento: “Del software utilizado, las normas y procedimientos implementados y a la acertada administración impulsada por el directorio, para fines de año se había incrementado el numero a 109 cajeros automáticos en plena función y más de 70 puntos en operación”.

Ramírez, C. (S/F), plantea que en Venezuela existe en la actualidad una base instalada de 6.200 unidades de cajeros automáticos aproximadamente, distribuidos por todo el país. Sin embargo, no existen estadísticas oficiales, lo que obliga a guiarse por las cifras que manejan los mismos proveedores de estos dispositivos.

En promedio un cajero en el país realiza entre 7.000 y 8.000 transacciones mensuales, aunque esta cifra puede llegar hasta 30.000 en algunos casos o también bajar hasta 2.000 o menos, como por ejemplo en los dispositivos instalados dentro de algunas empresas.

2.4 El Cajero Automático En Venezuela

La banca venezolana como en todos los países del mundo ha ido evolucionando hacia el negocio de prestación de múltiples servicios dentro de los cuales el sistema de pago personalizado está ganando terreno en forma significativa. En el caso venezolano, la reducción que en las últimas décadas han experimentado los índices de intermediación financiera, ha obligado a la banca a rentabilizar su negocio a través de la prestación de otros servicios que ha dado origen al concepto de banca personalizada.

Los cajeros automáticos surgieron en Venezuela a mediados de los años ochenta y constituyen un atractivo mecanismo ahorrativo de tiempo para los clientes y un instrumento para disminuir los costos en la gestión bancaria, con el ánimo de concretar la interconexión entre las redes y los cajeros operativos en el mercado venezolano, un grupo de bancos, entre los que se mencionan: Provincial, Venezuela, Caracas y Venezolano de Crédito, iniciaron conversaciones en 1987.

Según el análisis económico del servicio de cajeros automáticos realizado por la Gerencia de Estudios Económicos del Banco Federal en el año 2003, el crecimiento experimentado por los cajeros automáticos, entidades financieras afiliadas, número de transacciones y montos dispensados se ha expandido progresivamente en los últimos años, ya que en una economía como la venezolana, donde la demanda de dinero es cada vez más transaccional, se ha venido generando una recomposición de la liquidez monetaria a favor de instrumentos más líquidos (por la posibilidad de emitir cheques o hacer uso de las tarjetas de débito), que resalta el hecho de que los agregados monetarios circulante y del dinero tienen una participación cada vez más alta sobre el agregado liquidez monetaria 23,39%, en Agosto de 1993 a un 57,22% y al cierre de Junio del 2003.

2.5 Cajero Automático

"Es un equipo electrónico mediante el cual el cliente tiene la oportunidad de realizar diferentes operaciones financieras a través del uso de una tarjeta de débito o crédito, activada por claves secretas personales que permiten conectar al cliente con el computador central del banco". Grasso, V., J. (1998).

Según González Chávez, D (S/F), un cajero automático, "es un sistema automático computarizado con el que se maneja la recepción y entrega de dinero en efectivo; se pueden realizar consultas y también algunas operaciones".

Los autores antes mencionados, coinciden en que los cajeros automáticos son equipos electrónicos que permiten a los usuarios la facilidad de disponer de sus ahorros a cualquier hora del día sin hacer largas colas en los bancos, por medio del uso de una tarjeta con banda magnética la cual contiene toda la información del usuario. Este dispositivo electrónico permite realizar operaciones rutinarias por los

clientes del banco como lo son: retiros de efectivo, consultas de saldo, transferencia de saldo y estado de cuenta, entre otros. En otros países estos equipos pueden ser utilizados para efectuar depósitos a cuentas y pago de tarjetas o servicios básicos.

En conclusión, el cajero automático ha traído consigo grandes ventajas, agilizando las operaciones dentro de las instituciones financieras, y ahorro de tiempo por parte de los usuarios, así como también permitir a los bancos disminuir sus gastos por la contratación de personal para satisfacer la demanda existente y obtener beneficios económicos y financieros por el uso de los cajeros automáticos.

2.5.1 Características De Los Cajeros Automáticos

- Funciona las 24 horas del día.
- Permite realizar transacciones financieras sin tener que entrar a una agencia bancaria y desde cualquier sitio en que se encuentre un cajero automático.
- Permite realizar transacciones financieras con mayor rapidez y seguridad, brindando una mayor comodidad al cliente.

2.5.2 Componentes Del Cajero Automático

Un cajero automático se compone de:

- Un dispositivo para el reconocimiento y validación de billetes.
- Una computadora personal.
- Una pantalla (que también puede ser un monitor sensible al tacto).
- Un scanner para reconocer las tarjetas de débito o crédito con las que se entran al sistema con el que opera el cajero.
- Una impresora de comprobantes.

Su estructura la compone un gabinete exterior de lámina de acero con características y terminado “de uso rudo” (es decir, para ser utilizado por una gran variedad de personas un gran numero de veces),

para su instalación en el interior de un edificio o cubículo destinado para este fin. Cuenta con una caja fuerte para el resguardo del dinero en efectivo que reciben y que entregan, a la vez que está protegido con cerraduras de alta seguridad y llaves únicas.

2.5.3 Funcionamiento Del Cajero Automático

El cliente para realizar las operaciones en los cajeros automáticos, sólo necesita insertar su tarjeta de crédito o débito, marcando su clave o número de Identificación Personal (PIN), y seguir las instrucciones que aparecen en la pantalla y que paso a paso, lo llevarán a realizar las operaciones requeridas.

El PIN (Número de Identificación Personal), lo proporciona el banco al dueño de la tarjeta de manera confidencial, de tal manera que ni el mismo banco la conoce. En algunos otros casos es el propietario de la cuenta quien elige su número confidencial y lo activa personalmente, ya sea en la sucursal bancaria donde apertura su cuenta o por vía telefónica.

Existe una red de cajeros automáticos a nivel nacional, que le facilitan el uso de cualquiera de ellos independientemente del banco que le haya otorgado la tarjeta.

En la actualidad casi todos los bancos están afiliados a este sistema, pero para estar seguros, antes de hacer una operación, verifique que el cajero que pretende utilizar tenga en la puerta de entrada o en algún otro lugar visible el letrero “RED”.

2.5.4 Ventajas De Los Cajeros Automáticos Tanto Para Los Usuarios Como Para Las Instituciones Financieras

Las ventajas que ofrecen varían de acuerdo a las políticas de cada banco y al tipo de cuenta que cada usuario tenga. Sin embargo, las operaciones más frecuentes utilizadas por los usuarios son:

- Retiro de efectivo.
- Consulta de saldos.

- Consulta de últimos movimientos.
- Transferencia de fondos.
- Cambio de claves.
- Están disponibles al público las 24 horas del día, los 365 días del año.

Mientras que para las instituciones financieras las principales ventajas que le ofrecen los cajeros automáticos son las siguientes:

Es una forma económica de captar recursos; ya que generan un ingreso por cada transacción realizada, puesto que cada operación tiene un costo mínimo para el usuario.

Genera una notable reducción de costos a las instituciones en cuanto a la infraestructura, haciendo posible que el usuario efectúe sus transacciones sin la necesaria existencia de una agencia bancaria.

2.5.5 Desventajas De Los Cajeros Automáticos

- Son propensos a ser objeto de manipulación en sus componentes físicos; es decir, pueden ser modificados por los delincuentes adaptándoles dispositivos similares a los colocados por el fabricante y así cometer delitos sin que el usuario pueda darse cuenta.
- Como todo sistema informático o electrónico puede presentar averías; por lo general estas averías se presentan cuando los delincuentes introducen objetos para recabar información de bandas magnéticas de tarjetas de débito o crédito, dañándoles el lente óptico que es utilizado para la lectura de los códigos de las tarjetas
- Pueden presentar problemas de información o procesamiento de datos al momento de realizar una transacción; se asemeja al anterior, ya que pueda que el lente óptico haya sido dañado por la introducción de objetos para recabar información de tarjetas.
- Poseen teclados alfanuméricos muy grandes; que de una u otra forma permite que terceras personas puedan observar las transacciones realizadas por el tarjeta habiente evitando así la confidencialidad de la información realizada por el usuario.

2.5.6 Tipos De Cajeros Automáticos

2.5.6.1 Tipo Lobby:

Son aquellos que son ubicados en el interior de las oficinas bancarias o centros comerciales. La ventaja de este cajero es que es más seguro para los usuarios realizar las operaciones dentro de las oficinas del banco y en los centros comerciales, ya que los delincuentes no pueden visualizar las claves de acceso por las medidas de seguridad existentes dentro del local o las instituciones financieras, mientras que la desventaja para los usuarios es que este dispositivo electrónico se encuentra disponible en horarios de oficina.

2.5.6.2 Tipo Empotrable:

Son aquellos ubicados en las paredes adyacentes pertenecientes al propio banco. La ventaja de este cajero es que se encuentra disponible las 24 horas del día, mientras que la desventaja es que son propensos a que se cometan delitos con mayor facilidad.

2.6 Nuevas Tecnologías Para El Futuro

Con el fin de minimizar el índice delictivo en los cajeros automáticos, muchas empresas fabricantes de estos dispositivos han implementado nuevos sistemas de seguridad, para brindarles a los usuarios una mayor comodidad y confianza al momento de hacer uso de estos aparatos. Entre los nuevos sistemas de seguridad implementados a estos cajeros automáticos se encuentran:

2.6.1 Biometría De Huella Digital

Este sistema permite verificar la identidad del usuario mediante sus características físicas singulares.

Las compañías fabricantes de cajeros automáticos encontraron mercados incipientes para estas tecnologías en Sudamérica, donde los ciudadanos ya están habituados a identificarse por medio de su huella digital en sus documentos de identidad.

La compañía NCR instaló 400 cajeros con este nuevo sistema en toda la red del banco BanCafé, el quinto banco en Colombia, para brindar mayor seguridad a los colombianos y convencerlos así de que abrieran cuentas. De esa manera, el usuario no necesita una tarjeta de plástico, que atrae a los ladrones.

Prieto, R. (S/F), aseveró que “al principio éstos no reconocían las huellas digitales de clientes ancianos o con las manos encallecidas por el trabajo, tales como los obreros de la construcción”. Se mejoraron los sistemas de lectura, y el número de clientes con huellas ilegibles cayó del 30% al 8%.

2.6.2 Biometría De Identificación Por Iris

Este tipo de sistema es utilizado en aeropuertos de Canadá y Holanda para verificar la identidad de los pasajeros en la aduana y en retenes fronterizos de Emiratos Árabes Unidos para evitar que entren personas con visas de trabajo falsas.

La empresa fabricante de cajeros Diebold, ensayó cajeros con lectores de iris, pero los bancos no los adoptaron debido al costo y a que las cámaras son demasiado grandes. El usuario tenía que apoyar la nariz en la pantalla para que funcionara el lector.

Block, J. (S/F), asegura que “la verdadera meta de la biometría es terminar con el código PIN para que nadie tenga nada que robar”.

2.7 Delitos Informáticos

Según de la Luz Lima, M (S/F), define al delito informático en un sentido amplio “como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin”,

Según, el autor mexicano Tellez Valdez, J. señala que: "Los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

Por su parte, el especialista penal italiano Sarzana C., sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

En este orden de ideas, se entenderá como delitos informáticos todas aquellas conductas ilícitas susceptibles de sanción por el derecho penal, realizadas por individuos que hacen uso indebido de cualquier medio informático o telemático contra los derechos de los ciudadanos.

Los individuos o personas que cometen delitos informáticos, poseen habilidades y destrezas distintas a los delincuentes comunes, ya que manejan los sistemas electrónicos computarizados, y generalmente son individuos que su ambiente laboral está relacionado con los sistemas de procesamiento de datos, aunque se puede dar el caso de no ser personas que laboren en este medio; pero tienen los conocimientos sobre la materia.

En el transcurrir del tiempo se ha llegado a comprobar que los autores de los delitos informáticos son muy diversos, diferenciándolos entre sí la naturaleza de los delitos cometidos. El nivel típico de aptitudes del delincuente informático es tema de controversia, ya que para algunos su conducta no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico.

2.7.1 Características De Los Delitos Informáticos

Valdez, J. (S/F), plantea que los delitos informáticos presentan las siguientes características:

- Son conductas criminales de cuello blanco, que sólo un determinado número de personas con ciertos conocimientos pueden llegar a cometerlas.
- Son acciones ocupacionales, realizadas por sujetos que se encuentran trabajando en el medio informático.
- Provocan serias pérdidas económicas a los clientes y las entidades financieras, ya que casi siempre producen beneficios para aquellos que las realizan.

- Son muchos los casos que se conocen y pocas las denuncias realizadas por los afectados, y todo ello debido al desconocimiento de los ciudadanos de las leyes y normas que los regulan.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- A pesar de estar normado o regulados por la ley, estos delitos proliferan cada vez más, por lo que requiere de un mayor control por parte de las autoridades.

En la actualidad existen cientos de denuncias sobre retiros de fondos no autorizados por medio de la clonación de tarjetas de crédito y débito, además de montos desaparecidos de cuentas de ahorro y corriente a través de cajeros automáticos. En muchos de estos casos se presume que existe un porcentaje de complicidad interna de empleados bancarios, así como ciertas irregularidades y saboteos externos.

En los cajeros automáticos se registra la operación, e incluso dan el recibo del monto solicitado, pero no entregan el dinero ya que el dispensador no se abre. Técnicos especialistas que han sido consultados manifiestan que esto puede ocurrir, por desperfecto de la máquina, especialmente por falta de atención o mantenimiento, pero el banco está en capacidad y es su obligación saber exactamente cuanto dinero fue retirado físicamente y contrastarlo con el informe automatizado. A menos que un empleado deshonesto retire el monto en billetes sobrantes a la hora de chequear las operaciones.

2.7.2 Tipos De Delitos Informáticos

Las modalidades de fraude con tarjeta de Débito o Crédito son cada vez más extensas, por lo que se hacen necesario reagruparlas en tres (3) grandes grupos tomando como punto de partida el soporte o plástico con el cual se realiza la transacción.

Otro aspecto que se toma como referente para algunas clasificaciones es el “momento” en el cual se solicita la tarjeta a la entidad financiera, se entrega al usuario final, se utiliza en los cajeros automáticos y por último el momento en el que regresa a la entidad emisora.

Poveda, Nixon (2007), plantea: Entre las modalidades más frecuentes para cometer delitos en los cajeros automáticos y perjudicar de gran manera a los ahorristas y entidades financieras, se encuentran:

2.7.2.1 Fraude Realizado Con Tarjeta Autentica

2.7.2.1.1 Tarjeta Hurtada O Extraviada

Esta modalidad abarca el denominado “Cambiazo”, que es una forma de obtener la tarjeta de manera fraudulenta generalmente en los cajeros automáticos.

2.7.2.1.2 Utilización Indebida (Autoría Del Tarjeta Habiente)

Si es el mismo tarjeta habiente quien la utiliza y luego niega la transacción, se denomina autoría del tarjeta habiente, o si la presta a un tercero con la intención de cometer el fraude se trata de utilización indebida.

2.7.2.1.3 Tarjeta Emitida Con Documentos Falsos

La tarjeta se obtiene mediante el suministro a la entidad emisora de documentos e información de un ciudadano real (suplantación de persona) o inexistente.

En esta modalidad se hacen abonos a la tarjeta para generar saldos favorables; para que se configure el fraude debe existir la reclamación a la entidad financiera.

2.7.2.1.4 Suplantación Del Tarjeta Habiente En El Retiro Del Plástico

En esta modalidad el estafador en ocasiones con complicidad de funcionarios de la entidad financiera, retira una tarjeta suplantando al verdadero tarjeta habiente presentando documentación falsa.

2.7.2.1.5 Fraude Con Tarjeta Antes De Ser Entregada Al Titular

Se presenta con complicidad de funcionarios de la entidad financiera o por los proveedores que utilizan la tarjeta antes de ser entregada a quien la solicito.

En esta modalidad se puede presentar que la tarjeta autentica sea utilizada directamente en los cajeros, o por el contrario se copie la información de la banda magnética para luego ser manipulada.

2.7.2.1.6 Fraude Con Tarjeta Después De Ser Devuelta Por El Titular

Si no se siguen los procesos adecuados de control, custodia del plástico y destrucción del mismo, se facilita la utilización dolosa de la misma por el funcionario que la recibe ya sea de la entidad financiera o del proveedor.

2.7.2.2 Fraude Realizado Con Tarjeta Alterada

2.7.2.2.1 Tarjeta Alterada En La Banda Magnética

Son aquellos que se realizan a través de un cajero automático, utilizando plásticos en cuya banda magnética han grabado información de una tarjeta activa, o borrar y adicionar información en la banda magnética de una tarjeta de débito o crédito autentica.

2.7.2.3 Fraude Realizado Con Tarjeta Integralmente Falsa

Es aquel en el que se utiliza un soporte de características similares a los plásticos emitidos por las entidades financieras el cual es impreso, grabado y codificado con información privilegiada, simulando una tarjeta expedida por una entidad financiera.

Estas tarjetas son elaboradas en su totalidad por los estafadores sometiendo al plástico a procesos de impresión y realce de la información, y tiene como característica la falta de nitidez, de definición de color y ausencia de textos micros impresos en su mayoría.

2.7.2.4 Delitos Más Comunes

Dentro de los delitos informáticos que se cometen con más frecuencia en la actualidad en los cajeros automáticos según SUDEBAN son los siguientes:

En primer lugar se encuentra la **duplicación o clonación de tarjetas**, que se basa en la utilización de una máquina pescadora que copia la información de la banda magnética que tiene la tarjeta de crédito o débito.

Seguidamente se encuentra el **Phishing**, que es un correo electrónico fraudulento enviado por los delincuentes haciéndose pasar por uno legítimo de una organización especialmente instituciones bancarias, en el que los clientes son persuadidos a llamar a una línea telefónica directa.

En tercer término está el **Phishing telefónico**, en este caso los delincuentes realizan llamadas telefónicas haciéndose pasar como representantes de una organización especialmente instituciones bancarias, en donde los clientes son persuadidos a llamar a una línea telefónica directa, y de esta manera obtener información de cuentas y datos confidenciales por medio del engaño

En último lugar se sitúa el **jaqueo** realizado por personas que, por medio de sofisticadas artimañas electrónicas, acceden a las cuentas bancarias que les interesan y así cometen fraude por la vía electrónica.

Según la empresa de cajeros automáticos ATM, entre los delitos mas comunes que se cometen por los delincuentes informáticos se encuentran:

2.7.2.4.1 Lazo Libanés:

Éste instrumento tiene como función básica atrapar una tarjeta de débito o crédito. Los ladrones lo elaboran con una combinación de cartulina o plástico y cinta de video. Ésta va colocada en la ranura del cajero donde se introducen las tarjetas, y una vez pasada una tarjeta esta queda atascada o trabada y es aquí donde comienza la segunda fase de la estafa, en donde se acerca una persona ofreciendo ayuda al usuario y diciendo que a el le ha pasado el mismo problema, hablándole al usuario que marque un par de teclas y después el número de secreto de la tarjeta o (PIN). Mientras que el usuario realiza lo que le indica el estafador, éste mira por encima de su hombro para conseguir visualmente el código de seguridad. Una vez obtenido el mismo este le dice a la victima que se dirija al banco a informar de la

irregularidad, mientras que el cómplice del ladrón extrae todo el lazo (incluyendo la tarjeta) para cometer el delito en otros cajeros automáticos.

2.7.2.4.2 Pescadora:

Esta estafa comienza cuando los delincuentes colocan un lector de tarjetas de débito o crédito en la puerta de vidrio del cajero automático o en la ranura donde se introduce la tarjeta en el cajero automático. Con esto, copian la información de la banda magnética de la tarjeta. Una vez que la victima se encuentra adentro realizando la operación, para obtener la información de la clave de la tarjeta, colocan una mini cámara escondida en la parte superior del cajero, la cual transmitirá toda la información a una computadora que poseen los estafadores. Una vez obtenido todos los datos, los estafadores hacen una copia de la tarjeta que por lo general son hechas con llaves electrónicas de los hoteles, la cual poseen bandas magnéticas similares.

2.7.2.4.3 Doble Pantalla:

Este es otro de los trucos que se usan en los cajeros automáticos y a veces es casi imperceptible este aparato. Después que la victima introduce la tarjeta de débito o crédito y comienza a marcar el número secreto de su tarjeta o (PIN), seguidamente aparece en la pantalla un mensaje diciendo que la operación ha sido cancelada.

En realidad los datos que introdujo la victima quedaron registrados en la pantalla falsa. Los estafadores generalmente hacen esto en lugares poco iluminados. Después de obtener los datos pueden hacer una copia de la tarjeta

2.8 Caracterización Del Delincuente Informático

Luego de haberse examinado la definición de delitos informáticos, características, tipos de delitos, es muy importante señalar las particularidades del delincuente informático, debido a que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, que los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación

laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Las principales características que presentan los sujetos activos de esta conducta delictiva son las siguientes:

- En general, son personas que no poseen antecedentes delictivos.
- La mayoría de sexo masculino.
- Actúan en forma individual.
- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación “hackers”.
- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.
- En el caso de los “hackers”, realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovechan la falta de rigor de las medidas de seguridad para obtener acceso o poder descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.
- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).
- Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos

estudiosos de la materia lo han catalogado como “delitos de cuello blanco”, (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.)

2.8.1 Modus Operandi De Los Delincuentes Informáticos

Según informaciones recabadas en el CICPC de la delegación de Cumaná, señalan que las bandas de los llamados “Tarjeteros” operan con mayor frecuencia en los estados Nueva Esparta, Anzoátegui y Bolívar, así como también en los hoteles cinco estrellas de las grandes ciudades.

La razón es que en esos lugares es más probable encontrar un mayor número de usuarios de cajeros automáticos que posean tarjetas de débito y crédito con disponibilidades muy altas. Una vez obtenida la información sobre su cuenta los tarjeteros se dirigen a los cajeros automáticos utilizando como herramienta principal un aparato llamado pescadora, el cual es un pequeño dispositivo un poco más grande que una cajetilla de fósforos. Basta con deslizar la cinta magnética de la tarjeta de la victima para que quede registrada su información en la memoria de dicho dispositivo, luego con esa información usando una computadora y otro dispositivo sofisticado fabrica una cinta magnética idéntica a la de la tarjeta, colocándolo posteriormente en un plástico cualquiera (venta libre) para luego sustraer el dinero del cajero como si fuese el propietario de la cuenta, obteniendo así un lucro indebido.

Para efectuar los retiros de las cuentas de los usuarios, los tarjeteros están divididos en zonas de influencia, y atacan a las instituciones financieras cuyas tecnologías de información son más vulnerables. Estos delincuentes conocen las deficiencias en seguridad de la información de los bancos debido a que poseen contactos con empleados de los departamentos de sistemas, o trabajaron en ellos.

Un caso de estos delitos, es la de un experto en computación que presto servicios en un banco, renunció al cargo, pero antes de cesar la relación laboral sustrajo la información sobre los tarjeta habientes. Luego de usarla para enriquecerse, la vendió en dispositivos de almacenamiento masivo a otros delincuentes. El mismo grupo delictivo reclutó a un empleado de otro banco, y ocasionó una brecha de seguridad que les permitió sustraer cantidades millonarias a través de los cajeros automáticos.

.

A pesar del auge delictivo los bancos han implementado varias medidas de seguridad en los

sistemas de los cajeros automáticos solicitándoles a los usuarios de los cajeros más datos personales antes de entregar el dinero.

2.8.2 Técnicas Del Delincuente Para Clonar La Tarjeta Y Obtener La Clave O (Pin)

Una de las técnica más usadas por el estafador es cuando el usuario entrega su tarjeta para realizar un pago y la pierde de vista por algunos segundos, esto puede ocurrir en un restaurante mientras el mesonero lleva la tarjeta desde la mesa a la caja o viceversa, también ocurre cuando el cliente entrega la tarjeta y el dependiente del punto de venta trabaja en un mostrador alto donde no se puede ver sus manos mientras opera la tarjeta.

Cabe resaltar que si se trata de una tarjeta de crédito basta con la clonación porque no se requiere marcar ninguna clave para realizar un pago.

Otras técnicas muy usuales son las estafas en los cajeros automáticos, existen varias modalidades cuando el tarjeta habiente se dispone a usar su tarjeta en los cajeros: una de ellas consiste en que alrededor del cajero hay personas que se colocan detrás para poder observar cuando se marque la clave, posteriormente se apoderan de la tarjeta pretendiendo ayudar en la operación, tropezando, quemar con un cigarrillo o distrayendo la atención de cualquier forma; otra técnica igualmente sofisticada consiste en que los delincuentes colocan sobre la pantalla del cajero una pantalla falsa, cuando la victima introduce su tarjeta no lo hace en el cajero de verdad sino en el falso, dejando depositada la información de su tarjeta, luego cuando marca su clave lo hace en el teclado falso en cuya memoria queda depositada su contraseña.

2.9 Bases Legales

2.9.1 Legislación Comparada Sobre Delitos Informáticos

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, si bien es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, es por ello que se hace imprescindible que se siga trabajando para

llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Todo lo anteriormente señalado es corroborado por el brillante trabajo realizado en esta materia por la Organización de las Naciones Unidas titulado “El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos”, el cual señala que el problema se eleva a la escena internacional, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

2.9.2 Legislación En Venezuela En Materia De Delitos Informáticos.

Como se puede observar en el punto anterior se hace una breve mención de los países que legislan sobre la materia de delitos informáticos, así como, las organizaciones internacionales que han realizado esfuerzos dando sus recomendaciones para que se vaya adoptando una legislación uniforme en esta materia, particularmente la ONU. Ahora bien, dentro de este esfuerzo que se ha venido dando, tanto en el ámbito interno de cada país como a nivel internacional, para perseguir los delitos informáticos nos encontramos ante el caso de Venezuela que en los últimos cuatro años ha comenzado a legislar sobre este tema.

Dicho esfuerzo en Venezuela comenzó con la aprobación de la Constitución de la República Bolivariana de Venezuela, que establece en su artículo 110 lo siguiente:

Artículo 110.

“El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos

fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía".

El gobierno de Venezuela dando cumplimiento a la norma constitucional transcrita anteriormente, aprobó la Ley Orgánica de Ciencia, Tecnología e Innovación, que tiene por objeto tal y como lo señala su artículo1:

Articulo 1:

"El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional".

Sin embargo para que este esfuerzo de incorporar a Venezuela en la era de la tecnología y de la información, alcance un nivel adecuado, se hace necesario la promulgación de un conjunto de instrumentos legales que proporcionen el marco institucional al desarrollo armonioso del sector y a su democratización y, que precisamente para lograr los objetivos tanto de la norma constitucional como de la Ley Orgánica de Ciencia, Tecnología e innovación, se hizo necesario promover al mismo tiempo las condiciones de seguridad que inspirarán suficiente confianza tanto a los administradores de las plataformas que brindan servicios tecnológicos como al usuario en general.

Todas las leyes anteriormente señaladas han contribuido fundamentalmente a la incorporación de

Venezuela al desarrollo de la Ciencia y Tecnología de la información, y de esta manera adecuar su legislación en esta materia a las exigencias de la comunidad internacional. Pero así como se ha podido observar un gran desarrollo también hemos sido objeto de los daños y perjuicios que se producen a través de los delitos informáticos, es por eso que se tuvo que adoptar una ley en esta materia para que se facilitará perseguir este tipo de conductas antijurídicas.

2.9.3 Ley Especial De Delitos Informáticos

Esta novedosa Ley Contra Delitos Informáticos, aprobada a finales del año 2001, significa un gran avance en materia penal para el país, visto que permitirá la protección de la tecnología de la información, persiguiendo todas aquellas conductas antijurídicas que se realicen en este campo. Es por ello, que a continuación se señalan los aspectos más importantes de la ley:

2.9.3.1 Objeto De La Ley

El objeto de la Ley se encuentra consagrado en el artículo 1 el cual establece:

Artículo 1.

"La presente ley tiene por objeto la protección de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley."

Entre los artículos que se hacen referencia para controlar los delitos informáticos en los cajeros automáticos se encuentran:

Título II

De los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo nº 6

“Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias”.

Este artículo establece que toda aquella persona que viole la privacidad de la información de los cajeros automáticos, sin la debida autorización del usuario, mediante el uso de tecnología informática con fines lucrativos propios, serán sancionados de acuerdo a lo establecido en el artículo arriba mencionado.

Artículo nº 7

“Sabotaje o daños a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo”.

Se plantea en este artículo que quien realice sabotajes y altere el funcionamiento del sistema de un cajero automático, colocando objetos extraños e indebidos en los componentes del mismo con el objeto cometer actos delictivos será penado de acuerdo a lo establecido en este artículo.

Articulo nº 9

“Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas”.

El articulo establece que los delitos que se cometan violando las medidas de seguridad del los sistema protegido por claves de acceso, en el caso de los cajeros automáticos, pueden aumentar dependiendo del grado o magnitud del hecho, que perjudique a los usuarios de las instituciones financieras, bien sea persona natural o jurídica.

Artículo nº 10

“Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias”.

Establece que aquellas empresas o personas dedicadas a la venta de productos que puedan ser utilizados para fines delictivos como por ejemplo las pescadoras, tarjetas de plástico “vírgenes” y cualquier otro dispositivo o programa que contribuya a afectar a los usuarios de los cajeros automáticos por medio de la manipulación de sus cuentas, serán sancionados de acuerdo a lo descrito en este articulo.

Artículo nº 11

“Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenida en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado".

Este artículo especifica que todo aquel que obtenga y revele información contenida en los sistemas informáticos de las instituciones financieras a terceras personas para beneficio propio y de extraños perjudicando el patrimonio de los clientes o usuarios de la entidad y ponga en peligro la seguridad del Estado serán sancionados por lo establecido en el artículo.

Capítulo II
De Los Delitos Contra La Propiedad

Artículo nº 13

"Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

Establece, que todo aquel que se apodere de una tarjeta de débito o crédito, sin el consentimiento de su tenedor, para cometer delitos utilizando cajeros automáticos y beneficiarse económicamente, será penado por lo establecido en este artículo.

Artículo nº 15

"Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente

tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

Establece que aquellas personas que hacen uso de tarjetas de débito o crédito sin la debida autorización del titular para pórtalas, sean utilizadas para el pago de algún bien o servicio, serán sancionadas por lo establecido en este articulo.

Artículo nº 16

"Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere o duplique o elimine la data o información contenida en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte de los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema".

Establece que aquellas personas que manejen de manera fraudulenta tarjetas inteligentes, copiando, alterando y modificando la información contenida en estas, así como también aquellas personas o empresas que distribuyan material que puedan ser utilizados como instrumento para cometer actos delictivos a través de las tarjetas inteligentes, serán sancionados de acuerdo a lo establecido en este artículo.

Artículo nº 17

"Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta

inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlo a una persona distinta del usuario autorizado por la entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias".

Establece que aquellas personas que se apropien o utilicen una tarjeta de débito o crédito, la cual haya sido extraviada por una persona o canjeada a un usuario que haya utilizado un cajero automático con el fin de retenerlo y utilizarlo para cometer delitos, serán penados de acuerdo a lo establecido en este artículo.

Artículo nº 19

"Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias".

Establece que todas aquellas personas que posean equipos destinados a la falsificación, fabricación y distribución de tarjetas de debito y crédito, así como aquellas que realicen transacciones comerciales ofreciendo dispositivos que contribuyan o faciliten la realización de delitos a través de los cajeros automáticos, serán sancionados de acuerdo a lo establecido en este articulo.

CAPÍTULO III:
IMPACTO DE LOS DELITOS

3.1 Cuadro Comparativo Sobre Las Consecuencias Que Generarían Los Delitos En Los Cajeros Automáticos A La Institución Financiera Banesco, Usuario Individual Y Usuario Social.

Cuadro 1 Cuadro Comparativo Sobre Las Consecuencias Que Generarían Los Delitos En Los Cajeros Automáticos A La Institución Financiera Banesco, Usuario Individual Y Usuario Social

Banesco	Usuario Individual	Usuario Social
El capital de la institución se vería afectado.	Poco uso de los cajeros automáticos.	Generarían a la institución la perdida de grandes sumas de dinero.
Dejaría de percibir ingresos por concepto de comisiones en el uso de los cajeros automáticos por parte del usuario.	Eliminación de la tarjeta de débito de la cuenta, por miedo a ser victima de un nuevo delito.	Los usuario pueden verse afectado por la falta de información sobre las nuevas tecnologías y medidas de seguridad implementadas por las instituciones financieras.
Su reputación y prestigio se vería afectada por los usuarios.	Desconfianza de las nuevas tecnologías.	Al ser victima una gran cantidad de usuarios, aumenta la preocupación, disgustos y rechazo a los servicios que presta la institución.
Mayor congestionamiento de las sedes principales del banco para efectuar operaciones.	Preocupación y angustia por no saber el destino de sus ahorros.	Vulnerabilidad ante los Delitos Informático.

3.2 Impacto De Los Delitos Informáticos Tanto Para La Institución Financiera Banesco, Como A Sus Usuarios.

3.2.1 Impacto A La Institución Financiera

Los cajeros automáticos se han convertido en una valiosa herramienta tanto para la institución financiera como para el cliente, disminuyendo costos y realizando las transacciones con mayor comodidad y seguridad; además son fáciles de operar, ya que sólo basta con registrar el Numero de Identificación Personal (PIN) y elegir el tipo de operación de acuerdo a la necesidad del cliente en ese momento, proporcionándole al usuario la posibilidad de que en pocos minutos y en absoluta privacidad se puedan efectuar consultas de pagos, depósitos, retiros de cuentas, transferencias bancarias, entre otros.

En tal sentido, se observa que el futuro de los cajeros automáticos va en ascenso, ya que permite a las personas realizar un conjunto de operaciones, logrando así una novedosa alternativa de servicios bancarios a los usuarios.

En el caso de Banesco Banco Universal C.A. La implementación de los cajeros automáticos proporciona a la institución financiera, captar recursos económicos de forma rápida y a un bajo costo, siendo ésta una fuente de ingreso para el banco, por cada transacción realizada por los clientes debido al hecho de ser un servicio cómodo. Dicho dispositivo ha logrado que los usuarios sustituyan a las agencias, obteniendo las institución una notable reducción de costos en cuanto a infraestructura y tener mejor rendimiento en sus servicios, haciendo posible que el usuario realice sus transacciones en cualquier momento sin la necesidad de asistir al banco, siendo este responsable de estar a la par de la tecnología para ofrecer una mejor calidad de servicios, de modo que el público se sienta más a gusto.

El avance tecnológico ocurrido en los últimos años, ha generado un incremento considerable de los delitos informáticos, debido a que en la medida que se ha ido incorporando nuevas tecnologías en los cajeros automáticos, en la misma medida se ha observado una influencia de la delincuencia en la forma como se presta el servicio, la manera de cómo se realizan las operaciones y como ha afectado económicamente a la banca, ya que la institución financiera debe responderle a sus clientes aún cuando

el dinero se encuentra asegurado por la entidad, pero dicho seguro tiene como norma interna efectuar un deducible de los montos denunciados por los clientes el cual debe ser asumido por el capital del banco. Este deducible se realiza cuando el seguro comprueba que el número de denuncias por el mismo delito es elevado, lo que trae consigo desconfianza de la empresa hacia la institución, exigiéndole la cancelación de un porcentaje del total general del dinero denunciado.

Por medio de una entrevista realizada a la gerente de la sucursal de la Av. Bermúdez, Lic. Maria Gómez. Acotó que “una de las razones que ha generado el descontento de los usuarios hacia la banca, es el hecho de no responder a tiempo sobre la denuncia de delitos realizado en sus cuentas a través del uso de los cajeros automáticos, el cual se ha incrementado con el uso de esta tecnología, siendo motivo de preocupación, disgustos y hasta rechazo por parte de los clientes hacia el banco”.

La frecuencia con que se presenten los reclamos por concepto de delitos en los cajeros, es indicativo de la situación de aceptación de un banco en particular por parte de los usuarios, por lo que es indispensable verificar la gravedad del reclamo, realizando un seguimiento que verifique si es por situaciones nuevas o repetitivas.

En la actualidad los bancos deben definir claramente sus políticas en cuanto a la solución de reclamos de los usuarios por fraude y robo mostrando de esta manera la capacidad de las acciones que lo van a diferenciar de sus competidores, así mismo asegurar una respuesta rápida y solución satisfactoria al problema.

Las instituciones financieras, observan con interés las oportunidades que brinda la tecnología a sus propósitos de crecimiento y fortalecimiento económico. No obstante, el impulso hacia lograr el éxito y la preferencia del público, muchas veces se ve obstaculizado por los hacker informáticos en materia de delitos, llevando así a las agencias bancarias a realizar los cambios necesarios para alcanzar sus objetivos, invirtiendo grandes sumas de dinero en materia de seguridad informática para evitar la entrada en sus sistema y la obtención de los datos de sus clientes.

3.2.2 Impacto A Los Usuarios

El fortalecimiento y desarrollo de la tecnología, ha abierto infinitas posibilidades a los usuarios de realizar un sin fin de actividades de una manera rápida y fácil a través de los cajeros automáticos. La innovación a producido ciertos cambios de actitud en los usuarios, siendo estos tanto positivos como negativos, dentro de los positivos tenemos una gran aceptación y adaptación por parte de los clientes que no disponen de mucho tiempo y poseen conocimientos básicos bien sea suministrados por el banco o por personas cercanas a ellos, mientras que en lo negativo, esta presente el rechazo por algunos usuarios que carecen de cultura digital ignorando los beneficios que le pueden proporcionar los cambios tecnológicos, debido a los paradigmas existentes alrededor de esta tecnología, llevándolos a cometer errores que son aprovechados por los delincuentes, manteniendo a los canales tradicionales como los más confiables para los usuarios

La gerente de la institución financiera Banesco acotó que **"**Uno de los factores que ha afectado a los tarjetas habientes de la institución financiera al momento de hacer uso de los cajeros automáticos es la clonación de su tarjeta de débito o crédito, lo que trae consigo que sus cuentas de ahorros sean susceptibles a ser objeto de sustracción a través de este mecanismo por parte de los delincuentes".

Una vez que el usuario hace uso de su tarjeta en un punto de venta o en un cajero automático de la misma sucursal o de otro banco y se percata que ha sido victima de un delito electrónico, este se dirige a la institución financiera a formular la denuncia ante un promotor financiero sobre retiros no reconocidos, en donde se le suministra al cliente un formato o requerimiento para que especifique cada uno de los retiros que no reconoce, luego que el cliente llena el documento, la entidad financiera le exige entregar la tarjeta que fue objeto de delito y suspender temporalmente toda transacción con la misma, para luego encargarse de realizar un análisis o estudio en el sistema y verificar en que cajero fue cometido el hecho, cotejando si fue con la tarjeta original o con un plástico clonado.

Este procedimiento que realiza el banco en algunos casos es extremadamente engorroso para los usuarios, ya que el tiempo de respuesta en algunos casos ha durado desde 6 meses hasta 1 año, y por lo general, el tiempo de respuesta que ha establecido SUDEBAN a las instituciones financieras del país es de un máximo de 30 días continuos. En algunos casos las denuncias que realizan los clientes no proceden, generando malestar, inconformidad y hasta rechazo hacia el banco, procediendo el cliente a retirar su cuenta bancaria por miedo a que todo su dinero le sea robado.

3.2.3 Impacto A Nivel Social

La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de información sobre las nuevas tecnologías y medidas de seguridad implementadas por las instituciones financieras, lo cual lleva a que los usuarios se sientan inseguros y desconfiados a la hora de realizar sus transacciones bancarias a través de dispositivos electrónicos.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos en el sistema financiero público y privado del país, lo cual representa una de las principales preocupaciones que ha impulsado a la banca a tomar medidas urgentes para blindarse contra este delito.

Asimismo se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma negativa las oportunidades de trabajo para personas de este campo laboral.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquellas personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, entre otros.

La falta de cultura informática origina lo que conocemos como Analfabetismo Electrónico, es decir, la incapacidad de manejar las nuevas tecnologías por falta de conocimientos, ignorancia o exclusión, esto puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

En la actualidad existen organismos que están en la defensa del usuario cuando su denuncia es rechazada por el banco entre estos se encuentran la Alianza Nacional de Usuarios y Consumidores (ANAUCO), Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN), Instituto Nacional de Defensa del Consumidor y el Usuario (INDECU), los cuales servirán de intermediador entre el banco y el usuario y verificar los argumentos de la institución por el cual no procedió la denuncia.

Entre los delitos que no proceden por la institución bancaria Banesco, se encuentran:

- Cuando se efectúa el cambio de tarjeta (cambiazo).
- Cuando la tarjeta es utilizada por terceras personas (hijos, hermanos o padres).
- Cuando la cuenta sea mancomunada con firmas distintas y de los cuales los beneficiarios posean tarjetas de débito de la misma cuenta.

Con el fin de contrarrestar el auge delictivo en los cajeros automáticos, la institución financiera ha implementado una serie de cambios en estos dispositivos para mayor protección de sus usuarios, trayendo consigo que las personas se resistan a ciertos cambios, generando una barrera por la falta de conocimiento. Entre algunas de las causas que puede generar la resistencia al cambio se encuentra:

Lo desconocido provoca temor e induce resistencia; al no conocer cómo se utiliza cierto producto o servicio, se genera cierto rechazo a éste. El usuario desea sentirse seguro y saber que puede ejercer cierto control sobre las cosas que lo rodean; por lo general, al no conocer en que consiste el cambio se genera una resistencia, aún sin conocer los beneficios que le pudieran traer.

Aunque la tecnología facilita la realización de trabajos, transacciones, entre otros, muchas personas al no saber cómo utilizarlas, piensan que perderán tiempo o que podrán perder dinero, es por ello que se aferran a los procesos que siempre han utilizado, por el hecho de que tienen control sobre éstos y de alguna manera los hace sentir aptos para manejar su entorno.

El desconocimiento de la razón del cambio también genera resistencia; ya que una persona que

enfrenta un cambio tecnológico no sabe que es para su bien y que pudiera generarle beneficios, es por esto que aún muchas personas hacen largas colas en los bancos, en vez de realizar sus transacciones por el cajero automático, el cual le ahorraría tiempo.

La reducción de la resistencia al cambio puede alcanzarse por diversos medios; mientras más interactúe la entidad bancaria con sus clientes, más podrá entender las necesidades de ellos y ver así hasta que punto podrán aceptar los cambios, es por esto que la institución bancaria debe elegir alternativas que contribuyan a la aceptación del cajero automático por el usuario.

3.3 Medidas De Seguridad Implementada Por La Institución Financiera Banesco Para Contrarrestar Los Delitos En Los Cajeros Automáticos.

Los bancos saben que todo su prestigio se basa en la seguridad e integridad que brinden al dinero de los ahorristas. Es por ello, que ante la ola de fraude electrónico que azota a toda la banca nacional, han decidido tomar medidas de seguridad a corto, mediano y largo plazo.

A pesar de que los cajeros automáticos de la institución financiera Banesco no poseen mecanismos de seguridad físicos como por ejemplo cámaras de video para observar las aptitudes y movimientos de las personas: así como también no poseer protectores laterales y espejos de aumento para proteger al usuario cuando realiza las transacciones y observar a las personas que se encuentren detrás, actualmente se encuentran invirtiendo para reforzar su plataforma tecnológica por medio de nuevos sistemas de encriptación 3D o cajeros 3D, el cual trae consigo que no se pueda vulnerar una clave. La encriptación 3D, impide que un poderoso computador pueda descifrar una variedad de claves, por lo que requerirá más de un año tratando de decencriptarla, ya que éste diariamente esta cambiando sus código para impedir la obtención de información a personas ajenas al banco y por ende aliviar el problema que se tiene dentro de la institución financiera. Otra inversión que se encuentra realizando es por medio del cambio en el hardware, específicamente en el teclado del cajero automático, la cual será encriptada para que los delincuentes cuando ataquen a través de este medio no puedan obtener informaciones de las claves de los usuarios.

Esta inversión que realiza el banco Banesco, permitirá hasta cierto punto que el índice de delitos

electrónicos en los cajeros automáticos se minimicen, lo cual traerá consigo que los usuarios retomen la confianza en los servicios que ofrece el banco por medio de este dispositivo y por ende obtener los beneficios económicos que generan estos por su uso y aliviar aun más las agencias bancarias para disminuir costos de personal y poder realizar con mas calma los trabajos operativos referentes a la entidad financiera.

Según el Superintendente de SUDEBAN, manifestó que en los próximos meses todos los cajeros automáticos deben tener claves maestras individuales, de carácter secreto y confidencial. Así mismo, las llaves de trabajo o transporte entre cajeros automáticos y los bancos, y entre los bancos y redes, deben ser generadas de forma aleatoria; deben establecerse los procedimientos para garantizar el acceso seguro de los equipos por parte del personal autorizado por los bancos; y, por último, debe eliminarse el almacenamiento y registro de información sensible de archivos de los cajeros automáticos, o cualquier dispositivo que posea banda magnética.

En tal sentido, la institución financiera Banesco esta estudiando la posibilidad de introducir en el mercado unas tarjetas de débito y crédito por medio de un chip para sustituir las que poseen bandas magnéticas, y por lo tanto impedir que los delincuentes sigan cometiendo fraudes con las cuentas de los clientes, ya que la información que posee este tipo de tarjetas es muy difícil de acceder y codificar por medio de los mecanismos utilizados para clonar las tarjetas.

3.3.1.- Medidas De Seguridad

Entre las medidas de seguridad que recomienda la institución financiera Banesco para hacer uso de los cajeros automáticos en lugares concurridos como centros comerciales o instituciones financieras los usuarios deben tomar en cuenta lo siguiente:

- Sostener la tarjeta en la mano y no aproximarse a la máquina si se siente incómodo con la gente que esté alrededor.
- Si hay necesidad de utilizar los cajeros automáticos durante la noche, ir acompañado y dejar el automóvil lo más cerca posible.

- No aceptar ayuda de nadie, aunque la ofrezcan amablemente, ni cuando la tarjeta queda retenida en el cajero.
- En caso de cualquier incidente o duda acudir con los funcionarios de la sucursal del banco o reportar inmediatamente al teléfono de atención a clientes del banco.
- El Número de Identificación Personal (NIP) es la firma electrónica y no se debe suministrada a nadie.
- Utilizar una mano para digitar el NIP y la otra para cubrir el teclado a modo de evitar que cualquier persona vea la clave confidencial. Los empleados del banco no pueden ni deben solicitarle su clave confidencial en ningún caso.
- Memorizar el NIP y en caso necesario cambiarlo en el cajero si ha sido observado por otras personas.

CONCLUSIONES Y RECOMENDACIONES

Luego de haber desarrollado este trabajo de investigación, se observa que es posible mejorar la situación actual del servicio bancario en lo que a delitos informáticos se refiere tanto de la institución financiera en estudio como todas aquellas entidades bancarias que conforman la Banca Venezolana. Es por esto, que se señalan y resaltan a continuación algunas conclusiones y recomendaciones dirigidas a optimizar la calidad del servicio, incrementar la cultura digital y garantizar la seguridad, logrando que se mejore la relación cliente-banco y se fortalezca cada vez más con el paso del tiempo.

- Las operaciones bancarias deben ser ejecutas cuidadosamente puesto que mediante estas se cometen una serie de irregularidades generando por parte de los bancos preocupación, y en los usuarios mucha desconfianza e inseguridad al ver que el dinero puede ser plagiado y la privacidad interceptada por terceras personas que están vigilantes ante cualquier movimiento que se haga a través de los medios electrónicos con el propósito de copiar información y cometer delitos.
- La Negligencia e irresponsabilidad por parte de los usuarios a la hora de realizar las operaciones es el principal factor que conlleva o facilita la clonación de las tarjetas ya que por descuido o por falta de precaución los usuarios no protegen su clave a la hora de realizar las transacciones; Hoy en día la sociedad venezolana, carece de una cultura digital integral, ocasionando un obstáculo para que el cliente se desempeñe con eficacia dentro de la banca electrónica.
- Los delitos informáticos no solo se realizan en los cajeros automáticos, sino que también existen otros medios utilizados con el propósito de plagiar datos confidenciales de los usuarios e instituciones bancarias, como sustracción de la información a través de puntos de ventas, lector de tarjetas inteligentes, entre otros.
- La resistencia al cambio es un factor que las instituciones bancarias tendrán que tratar periódicamente; es decir, cuando existen cambios o nuevas modalidades en el país con respecto a un servicio, la mayoría de los clientes no las acepta con facilidad debido a que no les brindan toda la información correspondiente para que tenga confianza en el servicio que le ofrece el banco.
- Las nuevas realidades de la tecnología y la informática que se han venido desarrollando en este mundo globalizado debido a su acelerado desarrollo y su incidencia directa en varios ámbitos de la

sociedad han alcanzado el rango de bienes jurídicos protegidos por el ordenamiento jurídico, particularmente por el Derecho Penal. Por lo que una vez más nos hace pensar que estamos en presencia de un proceso de transnacionalización del Derecho Penal, donde gracias a la globalización se ha logrado realizar esfuerzos para la creación de un sistema capaz de proteger los derechos de la información de todos los ciudadanos.

Con la finalidad de evitar que los usuarios sean victimas de algún delito y este debidamente informado acerca de las medidas que debe tener en cuenta a la hora de realizar una operación en los cajeros automáticos, se presentan a continuación una serie de recomendaciones que deberían ser tomadas en cuentas por los tarjeta habientes como por la institución financiera

Recomendaciones para los Usuarios:

- Evitar ir a cajeros automáticos que se encuentren en lugares muy oscuros. Si no puede visualizar la operación que esta realizando, tampoco podrá identificar algún aparato extraño en el mismo.
- Antes hacer uso de un cajero automático, verificar que todos sus componentes están en su lugar y firmes y que no tenga cables raros o aparatos extraños pegados al mismo, de ser así dirigirse a la institución bancaria y denunciar la irregularidad.
- Cuando este en un cajero automático, desconfíe de cualquier persona que se acerque, ya que puede visualizar las claves de la tarjeta y toda la operación que realiza.
- Cuando vaya hacer uso de un cajero automático, cubra con el cuerpo o con las manos el código secreto o PIN de la tarjeta.
- Si la tarjeta queda trabada en la ranura del cajero automático, llamar al numero de servicio al cliente del banco (en lo posible no dejar el lugar). Cuando hable con un representante del banco, avisarle del problema y cancelar la tarjeta para evitar cualquier sorpresa desagradable; o si va acompañado de otra persona pedirle a ésta que se dirija al banco a informar la irregularidad.

Recomendaciones para la Entidad Financiera:

- El banco debe proporcionarle mayor seguridad a los cajeros automáticos, colocando protectores laterales para evitar que los delincuentes puedan visualizar el numero de identificación personal (PIN) de los usuarios. De igual manera colocar cámaras de seguridad para tener evidencia de los posibles delitos que se puedan cometer a través de los cajeros automáticos.
- La institución financiera debe adaptarle espejos de aumento en las esquinas superiores del cajero automático, para que de esta manera el usuario pueda visualizar a las personas que se encuentran detrás de él y observar sus aptitudes.
- Es recomendable definir claramente sus políticas en cuanto a la solución de los reclamos por parte de los usuarios victimas de fraudes y robo, para que el tiempo de respuesta sea más eficaz, mostrando de esta manera la capacidad de las acciones que lo van a diferenciar de sus competidores, y de esta manera dar solución rápida y satisfactoria al problema.
- Se recomienda realizar campañas para informar a los usuarios acerca del uso y beneficio de las nuevas tecnologías utilizadas para mejorar el servicio en los cajeros automáticos, de esta manera en cliente sentiría mayor confianza y así disminuir la resistencia al cambio por parte de los mismos.

GLOSARIO DE TERMINOS

Analfabetismo Electrónico: El analfabetismo electrónico hace referencia a la incapacidad de manejar las nuevas tecnologías por falta de conocimientos, ignorancia o exclusión.

Cracker: Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general causar problemas.

Estafa: Delito de apropiación patrimonial, en perjuicio de un tercero, realizado con ánimo de lucro y mediante engaño**.**

Fraude: Acto mediante el cual una persona, engañando a otra o aprovechándose del error en que se halla, obtiene ilícitamente alguna cosa o un lucro indebido.

Hacker: Es una persona que se interesa por el funcionamiento de cualquier sistema operativo para conocerlo mejor que quienes lo inventaron, sin causar daños físicos a personas sino burlar sistemas de seguridad que se encuentran inmerso en la red.

Hurto: Delito que comete el que se apodera, sin consentimiento, de una cosa ajena, con ánimo de lucro, sin hacer uso de la violencia**.**

Robo: El robo es un delito contra el patrimonio consistente en el apoderamiento de bienes ajenos, con intención de lucrarse, empleando para ello fuerza en las cosas o bien violencia o intimidación en las personas.

Tarjeta habiente: Es una persona que puede ser natural o jurídica, que posea una cuenta de ahorro o corriente en una entidad financiera y que realiza sus operaciones por medio de una tarjeta de débito o crédito.

BIBLIOGRAFÍA

Libros

Arias, F. (2006). El proyecto de Investigación: Introducción a la Metodología Científica. 5ta edición. Episteme: Caracas, Venezuela.

Ramírez, T. (1999). Cómo Hacer un Proyecto de Investigación. Editorial Panapo. Venezuela.

Sabino, C. (2002). El Proceso de Administración. Editorial Panapo. Caracas – Venezuela.

Trabajos de Investigación

Aguado, A. y Luna Y. (2007). Análisis de los Aspectos Negativos del Dinero Electrónico en las Transacciones Bancarias. Universidad de Oriente. Cumaná, Venezuela

Cordero, V. y Sifontes S. (2007). Banca Electrónica una Herramienta para el Desarrollo de Ventajas Competitivas. Universidad de Oriente. Cumaná, Venezuela.

Páginas Web

Aberle Y Cols, (1950) Disponible en: www.medmayor.cl/apuntes/apuntes/socioantropologia/z3GLOSARIO%20DE%20TERMINOS%20ANTROPOLOGICOS.doc

Anauco, técnicas de clonación. Disponible en: http://www.anauco.org/index.php?option=com_content&task=view&id=33&Itemid=29

ATM, tipos de delitos. Disponible en: http://www.univision.com/content/channel.jhtml?chid=9&schid=10294&secid=11428

Biblioteca Digital. Disponible en: bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/159/htm/sec_9.htm

Cajeros automáticos biométricos. Disponible en: www.magazine.com.ve/cienciatec/index.php?id=2009&idSec=11&accion=detalle

Definiciones en la Web. Disponible en: www.mundonotarial.com.mx/Notario/Glosario_2.htm
www.futurovenezuela.org/TH/glosario.htm
www.elgeomensor.cl/downloads/manuales%20y%20tutoriales/inde x.php
www.es.yourmoneycounts.com/ymc/tools/glossary.html
http://www.alegsa.com.ar/Dic/analfabetismo%20electronico.php

De la Luz Lima, M (S/F). Disponible en: http://www.monografias.com/trabajos17/delitos-informáticos/delitos-informáticos2.shtml

Delitos Electrónicos. Disponible en:
http://www.monografias.com/trabajos17/delitos-electronicos/delitos-electronicos.shtml

Delitos informáticos. Disponible en: http://www.tecnologiahechapalabra.com/datos/soluciones/implementacion/articulo.asp?i=1228

Diccionario Disponible en:
es.wikipedia.org/wiki/Robo

Golbano, J. Diccionario**.** Disponible en:
www.telefonica.net/web2/josegolbano/dicinfo.htm

Gómez Palacio, D. (2003). Disponible en:
http://www.elsiglodetorreon.com.mx/noticia/77609.muestra-debilidades-seguridad-bancaria.html

González Chávez, D (S/F) Disponible en:
(degonzal@correo.mty.itesm.mx)

Gonzáles, E. Análisis económico del servicio de cajeros automáticos en el sistema financiero venezolano. Disponible en: (www.eumed.net/cursecon/ecolat/ve)

Grasso V., J. (1998) La tecnología en la banca II. ENOL. Disponible en: http://iies.faces.ula.ve/investiga/chuecos/lecturas%20del%20seminario/unidad%20ll%5cll-1%5cgrasso%20v.,%20j.%20la%20tecnolog%c3%ada%20en%20la%20banca%20lll.doc

Ley Especial de Delitos Informáticos. Disponible en:
http://www.tsj.gov.ve/legislacion/ledi.htm
Pedra, M. Disponible en:
www.marcelopedra.com.ar/glosario_H.htm

Poveda D., N,(2007) Modalidades de Delitos. Disponible en:
Bogotá Colombianpoveda@incocredito.com.co

Ramírez, C**.** Banca Electrónica a alto ritmo. Disponible en: www.pcworld.com.ve/n118/articulos/informe4

Stav, J. La nueva Tecnología Protegerá tu Dinero
(Univisión-online, 29 de mayo 2007)

Hoja de Metadatos

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 1/5

Título	**Delitos Cometidos en los Cajeros Automáticos y su Impacto en los Usuarios y la Institución Financiera (Banesco) Sucursal de Cumaná, Estado Sucre. Durante el Periodo 2007-2008.**
Subtítulo	

Autor(es)

Apellidos y Nombres	Código CVLAC / e-mail	
ORTIZ SALAZAR, DAVID JOSE	CVLAC	16.084.560
	e-mail	Dosalazar82@hotmail.com
	e-mail	
ORTIZ ARCIA, JOSÉ RAMÓN	CVLAC	14.661.989
	e-mail	shamorro@hotmail.com
	e-mail	
	CVLAC	
	e-mail	
	e-mail	
	CVLAC	
	e-mail	
	e-mail	

Palabras o frases claves:

DELITOS
INFORMATICOS
CAJEROS AUTOMÁTICOS
CULTURA DIGITAL

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 2/5

Líneas y sub-líneas de investigación:

ÁREA	SUBÁREA
CIENCIAS ECONÓMICAS	CONTADURÍA
TECNOLOGIA	
ECONOMIA DIGITAL	

Resumen (abstract):

Todo organización empresarial, sea cual fuere su naturaleza, tiene dentro de sus principales objetivos lograr el mejor funcionamiento al menor costo posible. Dentro de este fundamento universal se inscribe el hecho que en la realización de las transacciones tradicionales del sistema bancario hay una lógica incidencia de costos. Al igual que otros sectores empresariales, las entidades financieras se han dedicado a la búsqueda de plataformas tecnológicas que le den posibilidad de expandir sus fronteras de servicios y negocios, con costos comparativamente accesibles y rentables, a la vez beneficiando a sus clientes o usuarios. En este orden de ideas, los bancos, mediante las Nuevas Tecnologías de Información y Comunicación (NTIC), tratan de incentivar novedosas modalidades de utilizar los servicios que estos ofrecen, esa mayor utilización de recursos tecnológicos se puede apreciar tanto en los bancos públicos como en los bancos privados. En tal sentido, el principal objetivo de este trabajo es observar y comparar cuales son las diferencias en cuanto a la aplicación de las NTIC entre la banca pública y la banca privada, en relación a los intereses y propósitos que cada tipo de organización manifiesta, en concordancia con su visión y misión de hacer banca, utilizando como marco inductivo el estado Venezolano. Para tal fin, se realizó una investigación de enfoque de campo en la que se acudió a dos instituciones bancarias privadas y a dos organizaciones bancarias públicas, en las cuales se aplicaron cuestionarios a parte del personal, y entrevistas no estructuradas a informantes claves. El trabajo aportó datos importantes para evaluar las diferencias en cuanto al uso, adopción, expectativas y aspectos legales, que posee cada tipo de banca y de que forma son beneficiados los usuarios-clientes.

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 3/5

Contribuidores:

Apellidos y Nombres	ROL / Código CVLAC / e-mail	
RAFAEL GARCIA	ROL	CA [ ] AS [X] TU [ ] JU [ ]
	CVLAC	10.462.247
	e-mail	Rafael@rjgm.net
	e-mail	
	ROL	CA [ ] AS [ ] TU [ ] JU [ ]
	CVLAC	
	e-mail	
	e-mail	
	ROL	CA [ ] AS [ ] TU [ ] JU [ ]
	CVLAC	
	e-mail	
	e-mail	
	ROL	CA [ ] AS [ ] TU [ ] JU [ ]
	CVLAC	
	e-mail	
	e-mail	

Fecha de discusión y aprobación:

Año	Mes	Día
2008	04	15

Lenguaje: spa

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 4/5

Archivo(s):

Nombre de archivo	Tipo MIME
Tesis_ortizyortiz	**Aplicación/word**

Alcance:

Espacial: Cumaná

Temporal: Años 2007-2008

Título o Grado asociado con el trabajo:

Licenciado en Contaduría Pública

Nivel Asociado con el Trabajo:

Licenciado

Área de Estudio:

Contaduría

Institución(es) que garantiza(n) el Título o grado:

Universidad de Oriente

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 5/5

Derechos:

Los autores nos reservamos los derechos de propiedad intelectual así como todos los derechos que puedan derivarse de patentes industriales o comerciales. Solo le damos el derecho de publicar el resumen de dicho trabajo.

AUTOR 1
Ortiz S. David J.
C.I: 16.084.560

AUTOR 2
Ortiz A. José R.
C.I: 14.661.989

JURADO 1
Prof. Rafael García.
C.I: 10.462.247

POR LA SUBCOMISIÓN DE TESIS: