Universidad Nacional de Loja

Facultad Jurídica Social Administrativa

Carrera de Derecho

"Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario"

Trabajo de Integración Curricular previo a la Obtención del Título de Abogado

AUTOR:

Juan Efrén Jumbo Condolo

DIRECTORA DEL TRABAJO DE INTEGRACIÓN CURRICULAR:

Dra. Gladys Beatriz Reátegui Cueva Mg. Sc.

Loja - Ecuador

2024

Certificación

Loja, 10 de diciembre del 2024

Dra. Gladys Beatriz Reátegui Cueva. Mg. Sc.

DIRECTORA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario,** previo a la obtención del título de **Abogado,** de la autoría del estudiante **Juan Efrén Jumbo Condolo,** con **cédula de identidad** Nro.**1104802440,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Dra. Gladys Beatriz Reátegui Cueva Mg. Sc.

DIRECTORA DEL TRABAJO DE INTEGRACION CURRICULAR

Autoría

Yo, **Juan Efrén Jumbo Condolo**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular, en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Cedula de Identidad: 1104802440

Fecha: 10 de diciembre de 2024

Correo electrónico: juan.e.jumbo@unl.edu.ec

Teléfono: 0960237857

Carta de autorización

Yo, **Juan Efrén Jumbo Condolo**, declaro ser el autor del Trabajo de Integración Curricular denominado: **Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario**, como requisito para optar por el título de Abogado; autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 10 días del mes de diciembre del dos mil veinticuatro.

Firma: 

Autor: Juan Efrén Jumbo Condolo

Cedula: 1104802440

Dirección: Calle Santa Rosa y Balsas, El Valle, Loja.

Correo Electrónico: juan.e.jumbo@unl.edu.ec

Teléfono: 0960237857

DATOS COMPLEMENTARIOS:

Directora del Trabajo de Integración Curricular: Dra. Gladys Beatriz Reátegui Cueva. Mg. Sc.

Dedicatoria

El presente trabajo de titulación lo dedico a mis queridos padres, Juan Segundo Jumbo Maza y Rosa Imelda Condolo Masache, quienes siempre estuvieron incondicionalmente pendientes de todo mi proceso de formación educativa, para llegar a ser un gran profesional, además por haberme forjado la persona que soy en la actualidad, me formaron con reglas y con algunas libertades, pero al final de cuentas, me motivaron constantemente para alcanzar mis anhelos.

Juan Jumbo Condolo

Agradecimiento

Quiero agradecer primeramente a Dios, quien me dio el don de la perseverancia para no rendirme y poder cumplir mis objetivos.

A mis queridos padres Juan e Imelda, quienes con su esfuerzo y sacrificio supieron apoyarme constantemente en este largo proceso.

A mis apreciados hermanos, Hernán, Franklin y Robalino que, con sus consejos, sus palabras de aliento me supieron motivar para no rendirme en buenos y malos momentos que se vivieron en el transcurso de mi carrera universitaria.

A los catedráticos de la UNL, que con el pasar de los años se convirtieron en un modelo a seguir para poder desarrollarme como un excelente profesional.

A la Universidad Nacional de Loja que me abrió sus puertas para forjarme como mejor persona y buen profesional.

A mi directora de tesis, Dra. Beatriz Reátegui por haberme brindado la oportunidad de recurrir a su capacidad y conocimientos; a la vez guiarme constantemente en todo el proceso de mi proyecto de titulación ya que sin su apoyo no hubiese logrado cumplir con los objetivos de mi proyecto.

Juan Jumbo Condolo

Índice de contenido

Índice de Tablas

Índice de Gráficos

Índice de Anexos

1. Título

Vulnerabilidad de la información a los usuarios basados delitos informáticos en el sistema financiero popular y solidario.

2. Resumen

Los avances tecnológicos y con ello la sociedad ha dado muchos saltos a lo largo del tiempo y a través de las diferentes herramientas y tecnologías que día a día se desarrollan se ha vuelto imposible el hecho que no se relacionen con la actualidad y sobre todo con el derecho, a lo largo del presente trabajo de investigación se realiza un muy pormenorizado análisis de los que respecta a los sistemas informáticos y sobre todo las vulnerabilidades que llega a presentar las plataformas de las diferentes instituciones bancarias, así como también la forma que estas mantienen para protegerse de cualquier ciberataque.

Se analiza a profundidad un marco teórico bastante amplio que abarca todo el tema del derecho penal como fuente de control y sanción a aquellas personas que atentan contra bienes jurídicos protegidos en el derecho ecuatoriano, además de ello se contempla el panorama claro de cuando se comete un delito informático, la forma de prevención y las diferentes falencias que pueden llegar a tener los sistemas informáticos, eso adicional al análisis de las normas internacionales de control de calidad y la manera en la cual se debe preservar la evidencia digital para evitar que esta pueda perderse.

Al ser un tema de interés social y abarcar principalmente al sector financiero del país se ha tratado de consultar a expertos dentro de la materia así como también funcionarios que laboran dentro de las instituciones bancarias, permitiendo de esta manera el análisis de su día a día en el ejercicio de la profesión; así mismo como es vital se ha trabajado con gerentes de Cooperativas de ahorro y Crédito, así como también trabajar en conjunto con la Fiscalía General del Estado y el Consejo de la Judicatura, mismos que a través de sus funcionarios de administración de justicia han logra solventar todas las dudas que se han devengado de la presente investigación.

Adicional para contar con un panorama real del tipo de delitos que se está trabajando se ha obtenido los datos estadísticos de los delitos informáticos directos y tipificados como tal, así como también aquello que si bien no se encuentran dentro de la categoría de delitos informáticos, se cometen a través de medios digitales, todo ello para culminar con una serie de reformas legales a la normativa y recomendar múltiples cambios en el tema de ejecución de investigación al momento de avocar conocimiento de un delito informático así como la creación de una unidad especializada para los mismos.

Palabras clave: ciberseguridad, vulnerabilidades, ciberdelito, integridad informática.

2.1. Abstract

Technological advances and with it society have made many leaps over time and through the different tools and technologies that are developed every day, it has become impossible for them not to relate to current affairs and especially to the law. Throughout this research work, a very detailed analysis is carried out regarding computer systems and, above all, the vulnerabilities that the platforms of the different banking institutions present, as well as the way they maintain to protect themselves. from any cyber attack.

A fairly broad theoretical framework is analyzed in depth that covers the entire topic of criminal law as a source of control and punishment for those people who attack legal rights protected in Ecuadorian law. In addition, a clear panorama of when a crime is committed is contemplated. computer crime, the form of prevention and the different flaws that computer systems may have, in addition to the analysis of international quality control standards and the way in which digital evidence must be preserved to prevent it from being lost.

As it is a topic of social interest and mainly covers the country's financial sector, an attempt has been made to consult experts in the field as well as officials who work within banking institutions, thus allowing the analysis of their day-to-day life in the exercise of the profession; Likewise, as is vital, we have worked with managers of Savings and Credit Cooperatives, as well as working together with the State Attorney General's Office and the Judiciary Council, which through their justice administration officials have managed to solve all the doubts that have arisen from this investigation.

Additionally, in order to have a real overview of the type of crimes being worked on, statistical data has been obtained on direct computer crimes classified as such, as well as those that, although not within the category of computer crimes, are committed through digital means, all of this to culminate with a series of legal reforms to the regulations and

recommend multiple changes in the subject of investigation execution when avowing knowledge of a computer crime as well as the creation of a specialized unit for the themselves.

Keywords: cybersecurity, vulnerabilities, cybercrime, computer integrity

3. Introducción

Las Tecnologías de la Información y en si todos los medios electrónicos han tenido una gran aceptación a lo largo de los años y con el transcurso del tiempo se han transformado en una herramienta de suma importancia para todas y cada una de las personas del mundo; partiendo desde una simple comunicación entre colegas mediante sistemas de mensajería instantánea; hasta poder elaborar transferencias electrónicas en tiempo real de valores monetarios a otra persona únicamente con la ayuda de sus dispositivos electrónicos; con ello es de destacar que día a día estos diversos sistemas informáticos son sometidos a constantes mantenimientos y regulaciones con la finalidad de evitar que la información que manejan de una u otra manera sea filtrada y puesta a manos de personas que pueden hacer un mal uso de esta información.

Con la finalidad de que el derecho avance en conjunto con los avances de la sociedad, el Estado ecuatoriano ha buscado proteger a los sistemas informáticos tipificando conductas penalmente relevantes para así evitar la impunidad de aquellos que vulneren la seguridad informática y buscar una reparación integral a los daños efectuados de acorde al bien jurídico protegido; es por ello que se han contemplado desde el Art. 229 al Art. 234.1 del Código Orgánico Integral Penal todos aquellos delitos contemplados como los ciberdelitos los cuales ataquen a los sistemas informáticos de una manera ya sea directa o indirecta; por lo que al ser relativamente nuevos su aplicación se ve en ciertos momentos limitados por los elementos del tipo penal para cada uno de ellos y así mismo por la falta de costumbre de aplicarlos.

En otra cara de la moneda nos encontramos con las Instituciones Financieras; tanto Bancos como Cooperativas en la actualidad y en base a la transformación digital han optado por crear plataformas propias o sub-contratar sistemas informáticos con los cuales poder otorgar a sus usuarios la facilidad de tener al alcance de su bolsillo el detalle pormenorizado de sus consumos con tarjetas; acreditaciones e incluso en ciertos casos poder acceder al

trámite de obtener anticipos de sus tarjetas de crédito a través de su plataforma de pagos; lo cual conlleva a que si bien el usuario tiene el libre acceso y mantiene a su disposición todos esa información; puede llegar a ser víctima de un delito informático por los llamados hackers; los cuales ingresan desde un usuario o dispositivo no autorizado y puede manipular la información de todos los usuarios del servicio.

Por ello, al ser una situación alarmante no solo para los usuarios sino que también una situación de especial cuidado para las diferentes instituciones públicas es de analizar las diferentes penas establecidas para estos tipos penales; así como también su aplicabilidad, concurrencia y sobre todo su competencia a la hora de poner en conocimiento de la autoridad legal correspondiente, resulta complicado por ser una tecnología que en el Ecuador no ha sido plenamente desarrollada; por lo que genera múltiples cuestiones por tratar, además de ello es de recordar que; en muchos casos estos delitos llegan a ser cometidos por grandes grupos de delincuencia organizada o personas que tienen su domicilio en otro país; por lo que es de analizar cómo evitar las posibles nulidades que puedan devengarse en el transcurso de la investigación y sobre todo; si las empresas del sector financiero se encuentran listas para sobrellevar cualquier ataque cibernético que puedan recibir no solo en la actualidad sino que también en un futuro.

4. Marco Teórico.

4.1. Derecho Penal

Para comenzar con el presente estudio, partiremos por el concepto del Derecho Penal; para Guillermo Cabanellas de Torres el derecho penal:

"(…) el Derecho Penal lo primero que ha de hacer es fijar los bienes jurídicos que han de ser protegidos penalmente y, sobre esos principios, variables en el tiempo y en el espacio, configurar específicamente los delitos y establecer la pena que a cada uno de ellos corresponde. (…)" (Guillermo Cabanellas de Torres; s.f., pág. 304)

De Cabanellas rescatamos que el derecho penal será aquel que fijara los bienes jurídicos objeto de protección y hace énfasis especial en los Principios los cuales amparan a este, para este autor el derecho penal es variable en relación al tiempo que transcurra y el espacio en el cual se desarrolle, además de aquello nos hace énfasis que este se encargara de configurar los delitos existentes y las penas, dando a entender que él se encargara que mantener el orden de la sociedad a través de reglas de convivencia aplicables para los ciudadanos.

De la misma manera, para Gómez y otros, en su libro Curso de Derecho Penal: Parte Penal manifiestan:

"(…) El Derecho Penal es el conjunto de normas jurídicas que definen determinadas conductas como delito y disponen la imposición de penas o medidas de seguridad a quienes las cometen. (…) Se trata de un sector homogéneo dentro del conjunto del Ordenamiento jurídico general especializado (…)" (Gómez et al, 2016, pág. 49)

En este punto varios autores coinciden en manifestar que el Derecho Penal abarca las normas que determinan las conductas del delito y la imposición de su respectiva pena por lo que esta garantizara de una manera tacita la seguridad de las personas de la sociedad.

Según Vaello citado por Rodríguez manifiesta que el Derecho Penal es:

"(…) Conjunto de normas jurídico-positivas, reguladoras del poder punitivo del Estado, que definen como delitos o estados peligrosos determinados presupuestos, asociando a las mismas penas, medidas de seguridad y otras consecuencias jurídicas. (…)" (Vaello, s.f., como se citó en Rodríguez, 2020, pág. 85)

Este autor incluye además ya al Estado con su poder Punitivo a la hora de desprender que es el Derecho Penal y coincide con los demás autores al manifestar que se trata del conjunto de normas que se encargaran de definir los delitos y sus presupuestos necesarios para su configuración, con la asociación de las penas correspondientes para la conducta desarrollada por el sujeto activo.

Para Wessels, Beulke y Satzger

"El derecho penal constituye aquella rama del ordenamiento jurídico que se vincula a infracciones jurídicas que han tenido lugar en el pasado, las cuales sanciona con pena; a través de esta se expresa a un juicio de desvalor ético-social frente al autor. Como manifestación del monopolio estatal de la fuerza, el cual excluye de venganza privada por el injusto, la persecución penal le corresponde al Estado como una tarea soberana. (…)" (Wessels, J., Beulke, W., y Satzger, H., traducido por Pariona Arana, R., (2018), pág. 1-2).

Estos tres autores alemanes presentan un concepto de Derecho Penal más simple pero preciso al momento de inducir de una manera tacita acerca del principio de legalidad e irretroactividad de la norma penal, pues por ese motivo habla de los hechos suscitados en el

pasado, buscando la sanción respectiva a través de la pena mediante un juicio, nos da indicios del debido proceso y la persecución penal por parte del Estado como una de sus tareas.

Con todo lo antes detallado destacamos que el Derecho Penal será el conjunto de normas las cuales, utilizando el poder punitivo del Estado, amparado en las normas de convivencia social, tipificará los presupuestos necesarios para la contravención de estas y así sancionar al infractor como velar por la protección de los bienes jurídicos tutelados y buscar la forma de resarcir los daños ocasionados.

4.2. Derecho Informático

"El Derecho informático como la rama del Derecho que regula los fenómenos provocados por la informática." Julio Téllez Valdés (2004: 21)

Entenderemos de tal manera al derecho informático como aquella la cual se centra y se desarrolla en todos aquellos elementos y situaciones devengadas por parte de las diferentes tecnologías que tiene determinada sociedad, de tal manera que con el derecho informático nosotros podremos controlar la situación jurídica de las redes informáticas y así poder solucionar los conflictos que se desarrollen por ello.

Por otro lado, para Aznit el derecho informático lo define como "el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información"

De tal magnitud que al momento de introducir principios en el derecho informático estamos hablando ya de una normativa no solamente orgánica, sino que también abordamos el dogma de la ley; en tal sentido que se buscara ponderar los derechos y las obligaciones de todas las personas que usan los medios informáticos para el desarrollo constante de sus actividades diarias.

Finalmente, como derecho informático por parte de Altmark encontramos que “es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática.”

Encontramos en este punto la correlación en instituciones de derecho y la existencia de la norma escrita, en tal sentido buscaremos que el derecho informático abarcara todos y cada uno de los temas que engloba la informática jurídica y que además de ello están plasmados en la normativa, abarcando así toda relación, ya sea de origen comercial o social que sea devengada gracias a la ayuda de las Tecnologías de la Informática

4.3. Informática Jurídica

Para muchas personas y conocedores del derecho muchas de la veces mal interpretan o confunden el concepto real entre la informática jurídica y el derecho informático; previamente se detalló que es el derecho informático; por consiguiente se deberá definir a ciencia cierta a que se refiere la informática jurídica, partiendo por la definición dada por Aznit encontramos que “es la ciencia que estudia la utilización de los recursos informáticos (hardware y software) para la mejora de los procesos (análisis, investigación y gestión) en el ámbito jurídico.”

En tal sentido encontramos pues que la informática jurídica es la forma mediante la cual diversos sistemas o personas que manejan a cabalidad esta ciencia pueden ocupar las diversas herramientas tecnológicas a su disposición para así obtener los resultados que desean, en ese sentido, la informática jurídica buscara una perfección en los procesos aplicados en diversas ramas del conocimiento apoyados siempre en las Tecnologías de la Información y Comunicación (TIC)

Otra definición que posee la misma valides la encontramos cuando revisamos y estudiamos a Fix mismo que afirma que “es el conjunto de estudios e instrumentos derivados

de la aplicación de la informática al derecho, o más específicamente a los procesos de creación, aplicación y conocimiento del derecho."

En ese sentido el autor nos confiere en este caso la aplicabilidad o utilidad de la misma, en tal sentido que esta sirve para que se pueda aplicar la informática de manera directa con el derecho, devengando de esa manera en una forma de mutualismo mediante la cual progresa y permite el avance tanto de la sociedad como de la administración de justicia. Por lo tanto y a criterio de este autor la informática jurídica confiere a todos los ámbitos del derecho las pautas necesarias y permite esparcir a través de los medios tecnológicos los conocimientos de derecho, facilitando tanto a los administradores de justicia como a los abogados en libre ejercicio el tener a su disposición y alcance todas las normativas que se requieran para tramitar sus casos.

Finalmente podemos rescatar la definición dada por Téllez, el cual la define como "la técnica multidisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación."

En tal sentido encontramos que se trata nada más que la manera mediante la cual se desarrollan los estudios en cuanto a derecho corresponden y la informática jurídica facilitara de una u otra manera que este estudio sea desarrollado de correcta manera, así mismo gracias a la informática jurídica se puede tratar la información, analizarla y buscar su recuperación manteniendo el respaldo electrónico correspondiente, facilitando al profesional del derecho el trabajar dentro de su campo de acción. Con ello ese llega a entender la relación que existe entre la informática jurídica y el derecho informático, llegando a un punto en el cual coexisten entre si y por lo tanto se apoyan mutuamente buscando siempre la relación mutua y

el progreso de ambas ramas, auxiliándose en aquellas diligencias y en las investigaciones más complejas a la hora de trabajar.

4.4. Seguridad Informática

La seguridad informática corresponde a uno de los principales pilares a la hora de determinar cuándo un sistema es el adecuado para poder ejecutar una función y además de ello dependiendo del tipo de sistema que nos encontremos manejando encontraremos con una u otra manera en la cual se proteja la información que estos contengan, en tal sentido la seguridad informática corresponde a uno de los pilares fundamentales a la hora de estudiar todo lo concerniente a la ciberdelincuencia en general; partimos por el concepto dado por Gómez (2006) el cual de una manera asertiva a definido a la seguridad informática "como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software."

La seguridad informática entonces será aquella que permitirá salvaguardar a los sistemas informáticos para así; poder garantizar su correcto funcionamiento y su correcto desempeño, además de aquello es de tomar en cuenta que gracias a la seguridad informática se evitan una gran cantidad de delitos, si las empresas no tomaran las medidas de actuación adecuadas para salvaguardar la integridad de los sistemas informáticos, entonces los usuarios mantendrían múltiples complicaciones a la hora de usar sus servicios electrónicos, provocando que se les genere afectaciones a su patrimonio e incluso que en ciertos casos estas afectaciones lleguen a dañar el sistema que mantiene una institución.

Otra definición de seguridad informática la encontramos dada por Kissel (2012) misma que la llega a definir como "la protección de información y sistemas de información de acceso no autorizado."

La seguridad informática en tal sentido se encargara de proteger a los sistemas informáticos del ingreso de personal que no se encuentre autorizado a acceder a determinadas herramientas del sistema, además de ello no solo llega hasta ese punto, sino que gracias a las medidas que son tomadas se puede verificar y dar un seguimiento de las actuaciones de cada uno de los usuarios y así en caso de detectar actividades sospechosas o poco comunes entonces podrá tomar las acciones necesarias para o bien retirar al usuario del sistema o solicitar una medida de autenticación o verificación de las acciones de los usuarios. De tal manera la seguridad informática es tomada para asegurarse de que el sistema que posee determinada empresa tenga las medidas necesarias para protegerse de algún ataque cibernético y con ello garantizar a sus usuarios que su información y sus datos personales se encuentran plenamente protegidos.

4.5. Políticas de control tomadas en el país.

El Estado ecuatoriano como mayor institución jerárquica en cuanto a la toma de decisiones dentro del país debe mantener seguros todos sus sistemas y proteger a cabalidad no solo a los usuarios de los mismos sino que esto abarca además la protección de los ciudadanos y su información que reposa en los registros tanto públicos como privados, como mayor institución en el país a través de sus diversos órganos ha procedido a ejecutar múltiples políticas para garantizar que esta información que reposa en las redes de datos no sean vulneradas.

Mediante Acuerdo Ministerial signado con el número 166 de fecha 19 de septiembre del año 2013, múltiples maneras en las cuales las instituciones gubernamentales procederán a proteger sus datos, destacando entre ello la necesidad de implementar la normativa INEN/ISO 27000 misma la cual se centra en la gestión de la seguridad de la información, buscando además que las instituciones principalmente gubernamentales implementen en sus

instituciones un Esquema Gubernamental de Seguridad de la Información o por sus siglas EGSI el cual garantiza la existencia del control de los datos gubernamental de las instituciones y se asegura que aquellos usuarios que tengan acceso a dicha información mantengan el control de los datos que son extraídos desde su sistema de redes de información.

El Esquema Gubernamental de Seguridad de la Información establece puntos importantes a ser tratados al momento de presentarse ante la autoridad, este esquema abordara los temas de políticas de seguridad de la información las cuales serán revisadas periódicamente con la finalidad de verificar su cumplimiento, así mismo implementa una organización para la seguridad de la información, momento en el cual la entidad gubernamental designara al encargado de la seguridad informática de la institución, siendo este quien deberá reportar cualquier anomalía que fuera detectada ya sea dentro del sistema o dentro de las actuaciones de los usuarios que acceden a él.

4.5.1. Política de control de acceso

En cuanto a las políticas de control de acceso conferidas por dicho acuerdo ministerial nos encontramos principalmente con tres:

a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados;

b) Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de la información; y,

c) Definir claramente los autorizadores de los permisos de acceso a la información.

Con estas tres políticas el estado lo que busca es principalmente que se mantenga un control por parte de la institución en cuanto a las personas que acceden a los sistemas de la información; y con ello en caso de una posible vulneración a la seguridad de los sistemas

actuar de manera correcta y neutralizar de ser necesario el usuario el cual está generando las afectaciones y vulnerando la confidencialidad de la información que tiene.

4.5.2. Política de uso de los servicios de red

Como política de uso de los servicios de la red de información el Acuerdo Ministerial a través de su anexo del EGSI establece a cumplir las siguientes políticas en cuanto a su uso de tal manera que se estructura así:

a) Levantar un registro de los servicios de la red la Institución

b) Identificar por cada servicio los grupos de usuarios que deben acceder

c) Definir los perfiles y roles por cada grupo de usuarios que tenga acceso a la red y sus servicios

d) Definir mecanismos de bloqueos para que sea restringido el acceso a los equipos de la red.

En cuanto a los servicios de la red de la institución tenemos claras las políticas a efectuarse en cuanto a la manera de acceder a los servicios de la red, identifica principalmente el servidor o usuario mediante el cual accede a diferente categoría de servicios, nos encontramos que para cada servicio tendremos un usuario destinado o su acceso será para ciertos servidores de la institución, atribuyéndoles dentro del sistema un rol especifico lo que les permitirá acceder o no al servicio, finalmente como política por parte de la institución se debe implementar un mecanismo de bloqueos que pueda ser usado en caso de inferir en una situación que comprometa a la red, en tal sentido estos bloqueos no permitirán que los usuarios sin autorización puedan acceder a la base de toda la información y alterar la misma.

4.5.3. Control de conexión a las redes

Como forma de controlar la conexión a las diferentes redes existentes dentro de la institución el Acuerdo Ministerial establece tres aspectos claros en cuanto a medidas que deberán ser tomadas por parte de la institución siendo estas las siguientes:

a) Restringir la capacidad de conexión de los usuarios, a través de puertas de enlace de red (Gateway) que filtren el tráfico por medio de tablas o reglas predefinidas, conforme a los requerimientos de la institución,

b) Aplicar restricciones considerando mensajería, transferencia de archivos, acceso interactivo, acceso a las aplicaciones, horas del día y fechas de mayor carga,

c) Incorporar controles para restringir la capacidad de conexión de los usuarios a redes compartidas especialmente de los usuarios externos a la institución.

Con esto lo que se busca es no solamente proteger a la red en general, sino que al limitar su acceso con la conexión mediante puertas de enlace o la transferencia de la información mediante sistemas de mensajería se asegura que este no llegue a las manos equivocadas, busca el limitar el acceso a redes externas principalmente para que estas no puedan ser objeto de hacking y con ello se obtenga las credenciales de acceso de alguno de los trabajadores de las instituciones. En tal sentido se ha buscado limitar el acceso a través de los mismos usuarios para así disminuir el riesgo existente entre la actividad laboral que desarrollan y la posible afectación a la red de datos.

4.6. Delito informático.

4.6.1. Evolución histórica.

Los orígenes de los delitos informáticos pueden rastrearse a partir de los años 60s por el temor infundido por la literatura de la época en relación a la recolección y almacenamiento de datos personales en computadoras. Éste tiene como referencia la obra “1984” de George

Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías. Tras la publicación de artículos periodísticos sobre algunos de los casos apareció por primera vez del término delitos informáticos o delincuencia relacionada con computadoras, retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como "ciberpunk". (Sain, G.; s.f.)

En cuanto a la historia de los delitos informáticos nos encontramos principalmente con los años sesenta principalmente inculcado a través de las obras literarias de la época, gracias a la transformación y la nueva implementación de tecnologías, en ese tiempo los fax y teléfonos, ante la idea de que una persona "controlaba" sus acciones a través de estos medios es que nace por primera vez el termino de delito informático o como delincuencia por medio de computadoras, siendo que este término en comparación con los otros tipos de delitos, es un término relativamente nuevo y que a su vez poco se ocupaba para esa época.

Durante los años ´60 en pleno Flower Power norteamericano, diferentes programadores o especialistas en informática intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio telefónico. El activismo político hippie de la época tuvo su costado informático a través de los phreakers (neologismo proveniente de las palabras en inglés freak, de rareza; phone, de teléfono; y free, gratis) donde a través de las llamadas blue box o cajas azules establecían comunicaciones en forma gratuita simulando los tonos de llamadas utilizadas por la Bell Corporation y la ATT, básicamente para comunicaciones de larga distancia. Con el correr del tiempo, estas técnicas de hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales. (Sain, G.; s.f.)

En esta época de la sociedad claramente al enfrentarse a una transformación digital se han cometido múltiples errores a la hora del acceso de las personas a los diferentes sistemas, careciendo de cualquier tipo de seguridad o de verificación, nacen las primeras iniciativas de transferir activos patrimoniales de cuentas bancarias para su beneficio propio, con esto además ya al empezar a establecerse las computadoras la principal manera de vulnerar sus sistemas físicos se trataba de extraer la información en pequeños componentes portátiles de almacenamiento de datos, por lo que, se mantenía aun una cierta relación directa entre la persona que ha cometido la actividad ilícita con aquella que manipula el ordenador o la información.

Ya durante la década de 1970 se comienzan a registrar una serie de casos que arrojan pérdidas cuantiosas para los sectores privados. A partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión. En relación al espionaje, estos se llevaban a cabo mediante la copia directa desde los dispositivos informáticos, el robo directo de los mismos para la extracción de información -discos duros, diskettes-, y la absorción de emisiones electromagnéticas para la captación de datos. Los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco espionaje industrial. (Sain, G.; s.f.)

A inicios de los años 70 podemos evidenciar que las personas las cuales requieren obtener cierto beneficio de los datos de otras personas o incluso de documentos que en esa época empezaron a respaldarse dentro de las computadoras, procedían a infiltrarse en donde reposaban estos documentos con la finalidad de obtener una copia de los documentos que requieren, con ello nos encontramos con los primeros indicios de delitos informáticos, pues

se han buscado beneficiarse del trabajo de otras personas y poder cometer otros delitos como lo son delitos contra la propiedad intelectual, en tal sentido, los delitos informáticos han comenzado a operar y desde entonces se perfeccionarían hasta alcanzar lo que conocemos en la actualidad.

A partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. Esto motivó la utilización por parte de las empresas emisores de la adopción de chips en los plásticos como medida de seguridad. Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial. (Sain, G.; s.f.)

En los años 80 nos encontramos principalmente con que estos delitos informáticos ya han progresado, de tal manera que se han establecido el fraude de las tarjetas de débito, debiendo así los Estados obligar a las instituciones a mantener chips para poder garantizar la personalidad de la persona que ejecuta la transacción además que con ello se ha potenciado en si la forma mediante la cual los diferentes países ven los delitos informáticos y como protegen a los usuarios de los abusos de los ciberdelincuentes, se empieza a perfeccionar las bases legales de las instituciones bancarias y demás empresas que se dedican a los negocios, principalmente por cuanto se busca proteger el robo de la información comercial.

Con la apertura global de Internet a mediados de los 90s por parte de la administración norteamericana y el posterior desembarco de las empresas y bancos a la red para el desarrollo del comercio electrónico, la preocupación central pasaba por el desarrollo de estándares de encriptación seguros para el desarrollo de operaciones financieras y la compraventa de productos en línea. Asimismo, la industria discográfica y cinematográfica comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor a partir de la descarga e intercambio en línea de música y películas bajo leyes de copyright, lo que generó un debate acerca de cómo concertar acciones de cooperación internacional para evitar fugas del negocio. La difusión de imágenes y/o ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad se empezaron a debatir mediante el uso de nuevas tecnologías. (Sain, G.; s.f.)

Con el avance de la tecnología es más que evidente la existencia de múltiples complicaciones y delitos informáticos cada vez más complejos, consistiendo en el ofertamiento de servicios sexuales de menores a través de los medios electrónicos como también la existencia clara de piratería de los productos audiovisuales como musicales, con ello los delitos informáticos se han establecido plenamente en los estados y por ende estos han procedido a formar parte del día a día de los ciudadanos, es de entender que esta producción o este trabajo ha llevado como consecuencia que los estados deban reforzar tanto sus conocimientos como también sus criterios a la hora de valorar la existencia de un delito informático.

4.6.2. Concepto y definición

Luis Camacho Losa (1987), define al delito informático como cualquier acción dolosa o culposa, es decir, con intención o sin intención, que cause daño ya sea a personas o

entidades de forma directa o inmediata a la víctima, haciendo uso de forma activa de dispositivos utilizados en las actividades informáticas.

Con esta definición obtenemos claramente el criterio de lo que significa un delito informático y con ello lo que devenga del mismo, en este caso deja en tela de duda el hecho de la intención en cuanto a la culpabilidad o que se trate de una conducta dolosa, pues en cierto punto esta acción puede devengarse a través de un dispositivo electrónico, por lo que permite facilita a las partes el poder definir o ejecutar las acciones que consideren necesarias para lograr su cometido final, sin tomar en consideración el daño que pueden llegar a generar.

Según Alberto Suárez Sánchez (2009), indica: En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información (págs. 44 - 45).

Con esta definición nos encontramos que no necesariamente el delito informático culmina al momento en el que se ejecuta la conducta delictiva, sino que además esta tiene que llegar a generar una afectación hacia los dispositivos de la información, en tal sentido que estos sufran una afectación ya sea en sus sistemas o en la ejecución de determinadas acciones informáticas.

Es importante señalar que las personas que cometen estos delitos, son conocedores de las tecnologías y sistemas informáticos, así como también, del comportamiento humano y organizacional (Enríquez Herrera & Alvarado Salinas, 2015)

Es importante el considerar lo último mencionado, pues es evidente que este tipo de conductas delictivas son cometidas por personas las cuales tienen un vasto conocimiento en lo que respecta a la informática, lo que les facilita de una u otra manera el acceder a estos sistemas para poder obtener la documentación que requieran u obtener el beneficio que se

encuentran buscando, así, su comportamiento y organización es evidente a la hora en la que se ejecuta, provocando muchas de las veces que este comportamiento devengado por los presuntos infractores, lleguen a generar afectaciones en el sistema informático y por ende perjudicar a los propietarios de estos.

4.6.3. El bien jurídico protegido

Por cuanto los delitos informáticos no solo atienden a un bien jurídico, sino que a su vez devengan de múltiples bienes afectados tenemos que tomar en consideración los siguientes criterios. La autora ecuatoriana Patricia Herrmann Fernández con referencia a la información como bien jurídico protegido en los delitos informáticos indica:

"El Derecho Penal por ser un derecho sancionador sólo puede actuar cuando se pone en peligro o se lesiona un bien jurídico. ¿Pero que es un bien jurídico? El bien jurídico según lo entiende la doctrina es siempre un interés vital, que no puede ser creado por el derecho sino por la sociedad de acuerdo a los valores vigentes en un tiempo dado. De acuerdo a esta noción hoy podemos afirmar que la información ha sido elevada a la categoría de un bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda sociedad. Esa es la noción de bien jurídico que sostenemos. Un bien jurídico novedoso, complejo que puede tener implicancias en lo económico, en la privacidad, en la seguridad y en otros órdenes, pero que no deja de ser la información como objeto del delito."

En ese sentido esta autora nos presenta la idea de la existencia de una complicación a la hora de definir el bien jurídico protegido, si bien esto dependerá en su mayoría de lo que determina el verbo rector, mismo que funge principalmente lo vital del verbo sancionador, es de tomar en consideración que estos también variaran dependiendo de lo que se encuentre tipificado en la norma, simplemente es de entender que es aquello que la sociedad como norma general buscara proteger y salvaguardar y que por lo tanto es con lo que se procederá a

trabajar en el caso de que se inicie una investigación por la comisión de un posible delito informático

del Pino y Páez Rivadeneira, con referencia a la libertad informática sostienen: “En conclusión podemos decir que el bien jurídico protegido de acuerdo con nuestra Constitución es la llamada libertad de informática la misma que consiste, como expresión de la libertad del individuo, en el derecho de utilizar lícita y libremente, con los límites constitucionales y legales la tecnología informática. Esto está dado en el reconocimiento de nuestra Constitución del acceso universal a las TICs por tanto a su uso libre.

En aras de buscar una explicación plausible y de acorde a lo que determina la norma estos autores contemplan que el bien jurídico protegido en los delitos informáticos no es más que la libertad informática que hasta en cierto punto tienen la razón por cuanto estos delitos afectan de una manera directa a la existencia de estos delitos, es de tomar en consideración además que la libertad informática es uno de los derechos que tienen los ciudadanos amparados en la libertad por lo que el estado debe mantener estas relaciones de una manera concreta y deben respetar la existencia de los mismo, por consiguiente, su bien jurídico protegido es la libertad informática.

Sin embargo, autores como Arias Torres manifiesta que no existe un bien jurídico protegido en el delito informático porque este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una protección específica en el Derecho Penal. Siguiendo esta línea de pensamiento se establecen como bienes jurídicos protegidos: el patrimonio en el caso de fraudes informáticos; la reserva y confidencialidad en el caso de delitos que afecten a la esfera de la intimidad; la fe pública en el caso de las falsificaciones.

4.6.3.1. Clasificación.

Según la empresa “Panda Security”; dedicada en su totalidad a proteger los diferentes sistemas informáticos y en buscar brindar ciberseguridad a sus clientes e usuarios en cuanto a la clasificación de los ciberdelitos nos entrega tres categorías las cuales se basan en la persona o el individuo que sufre la afectación, en tal sentido se tratan las siguientes:

4.6.3.2. Contra la propiedad.

Esta categoría de delitos son aquellos mediante los cuales el ciberdelincuente roba los datos de una persona o usuario concernientes a los datos bancarios, tales como contraseñas, tarjetas de crédito y débito entre otros, con ello se accede a los fondos de la persona afectada y procederán a realizar compras en línea o preparar estafas de pshishing con la finalidad de que la gente facilite su información personal, en este tipo de delitos también es muy común que se llegue a utilizar un sistema de software malicioso con la finalidad de conseguir los datos personales del dueño de las cuentas bancarias.

En esta categoría de delitos informáticos nos encontramos a una afectación al patrimonio de la victima de manera directa, pues se mantiene un registro electrónico de los consumos y transferencias realizadas por lo que de cierta manera la persecución de este tipo de conductas puede llegar a desarrollarse con normalidad, debido a la poca complicación que tienen; además de ello, es importante destacar que en este tipo de delitos informáticos muchas de las veces pueden llegar a ser capturados por el hecho de la simulación de la transacción o transferencia, siendo sancionadas de conformidad a las normativas legales de cada uno de los países.

4.6.3.3. Individual

La ciberdelincuencia individual es aquella en la que el presunto infractor procede a distribuir la información digital de una manera informal e ilegal, en cuanto a la ciberdelincuencia individual no encontramos principalmente con delitos como lo pueden ser

el cibercacoso, distribución o el mismo tráfico de la pornografía infantil, este tipo de delitos son cometidos de una manera directa por el ciberdelincuente y además de ello son trabajados por personas las cuales mantienen redes de comunicación de una manera anónima, pues así es la forma en la cual transmiten la información entre aquellos que la buscan y contratan sus servicios

4.6.3.4. Contra el gobierno

Uno de los ciberdelitos más Fuertes en cuanto a la vulneración de los sistemas informáticos, este tipo de delitos son aquellos los cuales atentan no solo ante la información del Estado, sino que además genera múltiples conflictos porque en ciertas ocasiones es considerado como ciberterrorismo, en este caso este tipo de ciberdelitos se dan en contra de los sistemas gubernamentales, aquí pueden ser el hackeo de los diferentes sitios web gubernamentales e inclusive a los sitios web gubernamentales. Esta categoría de ciberdelitos lastimosamente son los que mayor afectación generan en cuanto a los perjuicios que provocan no solo a los usuarios, sino que además generan la afectación al gobierno central, de tal manera que estos complican el actuar de las instituciones públicas.

4.7. Seguridad Bancaria en la actualidad

Las principales vulnerabilidades de la Banca Digital actual implican amenazas a la seguridad de los usuarios y del Entorno Financiero. Sufrir un ataque DDOS o ataque de denegación de servicio distribuido, es uno de los más comunes en la actualidad. Estos se producen cuando los servidores “se caen” y son ejecutados por Piratas Informáticos aficionados, por lo que protegerse es relativamente fácil. Otro de los métodos que ha tomado fuerza en este último tiempo son los ataques RansomWare, los cuales buscan conseguir el control del equipo, sea dispositivo móvil u ordenador, para cifrar el acceso al mismo, a su información y disco duro.

Frente a estas vulnerabilidades, es importante conocer todas las vías de la Ingeniería Social para evitar que nos infecten a través de engaños, es decir, el conjunto de técnicas que utilizan los cibercriminales para engañar a los usuarios. Es fundamental no abrir correos electrónicos de fuentes desconocidas y, en el caso de recibirlos, eliminarlos; utilizar enlaces de personas conocidas y confiables; mantener los Antivirus actualizados y utilizar contraseñas complejas de descifrar.

También es importante revisar el sitio Web de la Banca a la que accedemos, ya que las páginas oficiales cuentan con una serie de protocolos de monitorización de servidores que refuerzan y redirigen el tráfico de datos en caso de ser atascados, además realizan revisiones de evaluación de riesgos con el objetivo de mitigar cualquier problema.

4.8. Los delitos informáticos en la legislación ecuatoriana.

La existencia de los delitos informáticos en cuanto a la legislación ecuatoriana nos encontramos en dos momentos trascendentales a la hora de determinar cuánto ocurrieron o en qué momento fue que se comenzaron a sancionar.

a.- La expedición de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos publicada en el suplemento del Registro Oficial 557, de 17 de Abril del año 2002 normativa la cual por primera ocasión en el país se encargó de regular los medios electrónicos que estaban siendo utilizados, en ese sentido dentro de los diversos aspectos que fueron introducidos fue la incorporación de las infracciones informáticas en el Código Penal; legislación la cual regulaba todas las infracciones en el país, siendo estas posteriormente cambiadas por el Código Orgánico Integral Penal, lo cual nos lleva al segundo apartado

b.- La expedición del Código Orgánico Integral Penal – COIP- publicado en el Registro Oficial 180, de 10 de febrero del año 2014, conservo múltiples delitos que estaban tipificados en el Código Penal, además de ello tipifico nuevas infracciones, en especial

delitos contra la propiedad los cuales son por lo general los cometidos cuando se trata de un delito informático.

En la elaboración del presente trabajo de investigación los delitos que competen analizar son aquellos los cuales vulneran la seguridad de los sistemas en el tema de la banca, aun con ello analizare las infracciones que existían entre los textos del Código Penal y del Código Orgánico Integral Penal, partiendo de lo contemplado en el primer cuerpo legal mencionado para luego ubicar dichos delitos en el segundo y determinar cómo éste varió.

4.8.1. Delitos contra la propiedad

4.8.1.1. Apropiación ilícita por medios electrónicos

La primera de las categorizaciones que abarcan los delitos contra la propiedad es aquel que se contenía en el artículo que trataba de este delito en el Código Penal era la utilización fraudulenta de medios de información o redes electrónicas para facilitarse un bien ajeno. Nos encontramos con un verbo rector en el cual se busca la utilización de manera fraudulenta de diversos medios de la información, en ese caso el utilizar se entenderá como el emplear, usar, manejar, servirse, beneficiarse entre otros sinónimos; el sujeto activo o el presunto infractor en este tipo penal debería valerse de los sistemas de la información o redes electrónicas siendo estos aquellos mediante los cuales o bien sean dispositivos de almacenamiento de información o bien se tratase de los equipos interconectados entre sí de manera electrónica, buscando a través de ello apropiarse de los bienes ajenos.

Así mismo otro de los tipos que encontrábamos en el extinto Código Penal era el procurarse de la transferencia no consentida de los bienes, ya sea esto en beneficio propio o de una tercera persona, el verbo rector de procurarse significa o busca el intentar, pretender, esforzarse, acometer, emprender, entre otros, buscando como objetivo principal en este caso la transferencia de los bienes de una persona sin su consentimiento. Tanto en este tipo penal

como en el anteriormente detallado contemplábamos una pena privativa de la libertad seis meses a cinco años.

Posteriormente, con la entrada en vigencia del Código Orgánico Integral Penal estos verbos rectores serian contemplados en uno solo conocido como la apropiación ilícita a través de medios electrónicos, verbo rector contemplado en el Art. 190 ibídem, grandes cambios que contemplamos al momento del traspaso del verbo rector y de normativa es principalmente que ahora se contempla las telecomunicaciones y demás equipos de las terminales de comunicación, además de ser modificadas las penas privativas de la libertad pasando a ser de un año a tres años, por lo que estas fueron endurecidas.

4.8.1.2. Hurto o robo utilizando dispositivos electrónicos.

Este delito era contemplado por el antiguo Código Penal, en este caso era castigado única y exclusivamente si era cometido mediante la inutilización de sistemas de alarma o guarda, descubriendo o descifrando claves secretas o encriptadas; utilizando tarjetas magnéticas o perforadas; utilizando controles o instrumentos de apertura a distancia; y, violando seguridades electrónicas, informáticas u otras semejantes, mecanismos que no ameritan mayor análisis.

Este delito en el Código Orgánico Integral Penal desapareció como un delito independiente, siendo agregado como un inciso del Art. 190, por lo que principalmente encontramos que se elimina por completo la palabra del hurto o robo, siendo este tipo penal trabajado en conjunto al Art. 190. En este aparto no existe mayor caso a analizar, pues principalmente al desaparecer el verbo rector anterior no amerita que sea mayormente profundizado.

4.8.1.3. La estafa informática

En este caso en especial en el Código Penal el delito de estafa informática no poseía mayor relevancia, pues principalmente no encontramos un verbo rector especialmente dedicado a este, en este caso simplemente se limitó a determinar que en caso de la utilización de un medio electrónico o telemático se aplicara la pena máxima para el caso de la estafa, en este caso se buscaba la apropiación de un bien ajeno a través de engaños.

Para el actual Código Orgánico Integral Penal nos encontraremos principalmente con que de igual manera no se tipifica como estafa informática, sino que en su lugar encontramos como una condicionante para que el delito sea sancionado con la pena máxima los siguientes tipos o condiciones:

"1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.

4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.

5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor." (Código Orgánico Integral Penal; 2014, última reforma 2024)

Principalmente en estas características si bien afectan a los usuarios de la banca, estos delitos conllevan la existencia de un documento físico anterior, buscando además en este tipo el abarcar el tema de la defraudación por lo que de cierta manera no está adecuadamente tipificado, esta característica provocaría en cierto caso que se generaran errores al momento de adecuar el verbo rector.

4.8.2. Delitos contra la fe publica

4.8.2.1. Falsificación electrónica

En el Código Penal este tipo penal era considerado como una falsificación de documentos en general, La finalidad del cometimiento de esta clase de delitos no solo era el ánimo de lucro al igual que en los delitos de apropiación ilícita sino el simple interés de causar daño o perjuicio a un tercero configuraba el delito. El medio empleado podía ser cualquiera. Las formas de cometimiento del delito eran la alteración; modificación; simulación; o suposición, todos verbos que suponen un cambio material de algo existente o la creación de algo parecido a lo que ya existe.

En el actual Código Orgánico Integral Penal este tipo penal fue suprimido por cuanto este ha tratado de ser suplido por nuevos tipos penales o ser adecuado en otros tipos, lo cual a mi criterio ha dejado en desprotección a los sujetos pasivos del cometimiento de este delito, dejando en múltiples casos a estos sin protección lo que conlleva que no tengan pleno acceso a la justicia.

4.9. Modalidades de Delitos Informáticos.

Los delitos informáticos no solamente afectan a los bienes jurídicos tendientes a la propiedad de las personas, estos atentan además contra la información que tienen los usuarios dentro de las diferentes instituciones bancarias la cual goza de sigilo, por lo que no puede ser divulgada bajo ninguna circunstancia; ante esta situación dentro de lo que conocemos como

el Código Orgánico Integral Penal no encontraremos el desarrollo real de los términos existentes para la comisión de los delitos informáticos, por ello explicaremos uno a uno en cuanto a su definición, que abarca y cuáles de estos son los que con mayor frecuencia se dan:

4.9.1. Phishing

El termino Phishing fue creado aproximadamente en los años 90, proveniente de una palabra en el idioma inglés "fishing", cuya traducción literal es pesca, lo que significa en si es adecuar la conducta de una persona la cual realiza determinada acción y se pretendía que el dueño de una cuenta muerda el anzuelo. Este término puede llegar a abarcar correos electrónicos falsos, mensajes fraudulentos mediante los cuales se buscará engañar al usuario con la finalidad de obtener contraseñas, datos bancarios, e inclusive en ciertos casos información personal o delicada como puede ser el domicilio entre otros.

Páez y Acurio lo llegan a definir como "el uso no autorizado que un tercero hace de los datos que identifican a una persona con el fin de defraudar o cometer otro delito con una motivación financiera." Es decir, lo que se pretende mediante esta modalidad de comisión de ciberdelito es principalmente ejecutar acciones dentro de una cuenta virtual como si se tratase del titular, con ello tienen a su disposición la información del usuario y por consiguiente pueden hacer lo que creyeran conveniente.

Por otro lado, Arcilla lo define como "un acto que tiene por objeto lograr que la víctima revele información personal o confidencial.". mediante esta modalidad la información personal de los usuarios juega un papel fundamental a la hora de poder acceder a los sistemas informáticos y en si a las bancas virtuales, con ello el ciberdelincuente procederá a extraer toda la información que deseare y poder hacer el uso que más le creyera conveniente en base a sus intereses, lastimosamente hasta cierto punto el phishing puede llegar a ser en su totalidad responsabilidad de la persona o del usuario, pues es el de manera directa quien cae

en la trampa, aun con ello la institución financiera deberá buscar la forma mediante la cual el usuario aprenda acerca de esta modalidad y que no se entreguen los datos personales como lo son claves o números de tarjetas a través de los medios telemáticos.

4.9.2. Pharming

Según el sitio web de ciberseguridad "Kaspersky" define al pharming como una combinación entre lo que es las palabras "phishing" y "farming" el cual "es una estafa en línea similar al phishing, en la que se manipula el tráfico de un sitio web y se roba información confidencial." Esta modalidad de ciberataque tiene la función de redirigir a los usuarios del internet que buscan ingresar a un sitio web en específico, para que accedan a otro diferente y falso, principalmente se trata en ese sitio el extraer la información de los usuarios, por lo general puede llegar a darse con páginas web similares a las de las bancas virtuales de sus instituciones bancarias, con ello al apropiarse de esta información, pueden no solamente descargar programas los cuales puedan afectar el buen funcionamiento del equipo tales como virus o troyanos.

Páez y Acurio lo define como el "ataque a los computadores personales que consiste en modificar o sustituir el archivo del servidor de nombres de dominio (D.N.S) cambiando el IP real de la entidad bancaria para que al escribir en la barra de direcciones el nombre de dominio de la entidad, el navegador nos dirija a la dirección IP donde se aloja la página falsa de esa entidad en la que se recogerán claves de acceso de los clientes.". por tal motivo el farming es un proceso más intrusivo en el equipo de la persona de mantiene la información, de tal sentido que para que pueda llegar a darse esta situación es necesario que el usuario previamente haya accedido a direcciones web que no sean seguras o que haya expuesto su dispositivo de una manera u otra en las diferentes plataformas digitales.

4.9.3. Rounding of Utility

Modalidad de ciberataque en la cual se ataca de una manera directa y más intrusiva en los sistemas electrónicos de las diferentes instituciones bancarias, según Páez y Acurio "Consiste en redondear céntimos en determinadas operaciones bancarias para luego depositarlas en cuentas propias." Principalmente en esta modalidad de ciberataque ya el ciberdelincuente debe tener acceso directo al sistema de la institución bancaria, bajo esa premisa aquí la relación y responsabilidad de la banca puede estar estrechamente relacionada, es de entender además que este tipo de delito no es necesariamente una afectación mayoritaria a las personas que sufren dicho ataque, pues la cantidad descontada de sus cuentas bancarias es tan baja que en muchas ocasiones ni siquiera se percatan que se ha efectuado, más para el ciberdelincuente si existe un beneficio más grande, para ejemplificar de mejor manera, si a una persona le debitan 1 centavo de su cuenta bancaria, pocas veces lo notara e inclusive si lo llega a notar no tendrá una mayor preocupación, pues supondrá que se trata del costo de algún mantenimiento al sistema de la misma banca, pero para el ciberdelincuente no solamente descuenta a una persona sino que se los descuenta a todos los usuarios de una institución, de tal manera que 1 centavo multiplicado por 1'000.000 de usuarios llegan a significar 10.000 dólares para el ciberdelincuente, el cual esperando un poco de tiempo puede volver a efectuarlo sin que los usuarios se den cuenta de esto, generándole afectación a la banca.

4.9.4. Caballo de Troya

Esta modalidad de ciberataque consiste principalmente en disfrazar un programa como otro, este nuevo programa lo que hace es "modifica(r) las instrucciones a un programa informático ya existente, insertando nuevos programas o nuevas rutinas a fin de obtener resultados distintos a los previstos en la configuración inicial del programa para realizar una función no autorizada" (Salamea, p. 83) con ello se insertan programas distintos a los que el

usuario tenia pretendido instalar y procederán a extraer la información que requieren en cuanto a los datos personales e inclusive activar las cámaras y micrófonos de los dispositivos.

El mismo autor lo expresa de la siguiente manera “un caballo de Troya informático entra en el sistema de forma aparentemente inofensiva (un archivo adjunto en un mail, un juego que te copia un amigo, etc.) y una vez dentro se activa, y se convierte en una herramienta, que, desde dentro, abre todas las puertas para que el atacante pueda tomar control total del sistema” este modo de operación permite al ciberdelincuente tomar en su control a todos los usuarios que han tenido dicho programa, por lo que claramente extrae la información personal de este y le da un mal uso, puede dañar el equipo del usuario, puede inclusive llegar a extraer la información de este y con ello hacer y deshacer lo que quiera, sin siquiera que se puedan percatar que esto está sucediendo.

4.9.5. Hacking

Para Hermann el hacking es el “acto de mero acceso o permanencia perpetrada con el fin de vulnerar un password o una puerta lógica que permite acceder a sistemas informáticos o redes de comunicación electrónica de datos” Esta modalidad de operación consiste en entrar de una manera no autorizada o poco común a los sistemas informáticos, en los cuales se pretende ya sea vulnerar los códigos del sistema o extraer información de los mismos, dentro del hacking nos encontramos curiosamente con una modalidad la cual incluso es empleada por distintos informáticos de una manera ética o para reforzar las medidas de seguridad, con ello se contrata una persona a fin de que busque la forma de ingresar mediante al hacking a los sistemas informáticos y en caso de lograrlo demostrar la inseguridad existente para poder reforzarla, prácticamente consiste en un trabajo en el cual se pretende buscar la mínima vulnerabilidad y a raíz de ella eliminar o efectuar el daño a los sistemas informáticos.

Para concretar este tema Lucena define el hacking como algo más sencillo, siendo únicamente “la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes”, por lo que el hacking tal y como lo hemos detallado no necesariamente tiene porque actuar de una manera dolosa, pues existen casos en los que estas técnicas de búsqueda de vulnerabilidades son contratadas por las mismas instituciones bancarias las cuales buscaran reforzar la seguridad de sus sistemas informáticos, claramente para la ejecución del hacking es necesario que la persona que lo realiza tenga un amplio conocimiento en las materias de la informática y conozca muy bien las vulnerabilidades de los diferentes sistemas informáticos, por lo que su ejecución es mucho más limitada, así como también su frecuencia, pero una vez que se logra concretar la acción y se logra acceder al sistema los daños que pueden generar son extremadamente amplios.

4.9.6. Key Logger

Para el sitio web de ciberseguridad llamado “Kaspersky” nos menciona que “Los keyloggers están diseñados para generan registros de todo lo que escribes con el teclado el de una computadora o un dispositivo móvil.” Principalmente de estos archivos podemos obtener que trabajan como un registro ya sea digital o físico de todo aquello que es escrito dentro de un ordenador o dentro de un dispositivo móvil, cabe destacar que estos pueden ser legales e ilegales, por ejemplo, legales cuando uno trabaja en determinada empresa en la cual se maneja información con cautela o para controlar los datos y mensajes que son escritos dentro de un dispositivo e ilegales cuando estos son instalados sin autorización y por ende mantienen un registro ilegal, estos archivos o dispositivos principalmente trabajan con la finalidad de obtener las credenciales de los usuarios y por ende, con un poco de trabajo obtener la información que requieren para poder extraer los bienes de las personas.

El Banco del Pacifico, define un key logger como “herramientas de software o hardware que permiten grabar el texto que escribe una persona en su teclado. En el caso del

software, el key logger captura todo lo que escribe la víctima y lo envía a una dirección de correo electrónico configurado por el delincuente. Estos programas se instalan y funcionan de manera invisible" por lo que no existe una manera salvo un antivirus o mantenimiento constante mediante el cual percatarse de la existencia de uno cuando se trata de software, en el caso de que este sea a través del hardware; es más sencillo percatarse de uno de estos equipos, principalmente porque son adjuntados como USB ubicados por lo general entre la pantalla y el monitor, con ello registra todas las teclas que son pulsadas por la víctima y a través de eso obtener las credenciales de acceso a diferentes plataformas.

4.9.7. Data Diddling

Este modo de operación es un tanto complejo de explicar por lo que nos apegaremos a lo que manifiesta Paez y Acurio por lo que "el autor del delito realiza una manipulación del computador, sistema o red con la finalidad por ejemplo de que un comando del ordenador realice otra función para la que estaba prevista como el borrar archivos o crear identidades falsas, este es el tipo de técnica que se utiliza para derivar fondos de diversas cuentas a una cuenta determinada."

El actuar mediante esta manera implica la participación directa de la persona la cual esta cometiendo el delito, pues se infiltra dentro del mismo y procederá a manipular la información del usuario con la finalidad de desviar las operaciones u transacciones que este realice, por lo que una vez más es posible que la víctima no reconozca siquiera que está sufriendo un ataque a su sistema o si equipo y por ende no pueda realizar ninguna acción con la finalidad de frenar la ejecución del hacker.

4.9.8. Cloning

Esta modalidad de ciberdelito es conocida por operar directamente con las tarjetas de crédito o débito de los usuarios de la banca, principalmente este delito se caracteriza por

trabajar en coordinación con los empleados de determinados locales comerciales, estos al momento de recibir la tarjeta del cliente, ya sea débito o crédito proceden a clonarla utilizando un mecanismo especializado para duplicar las bandas magnéticas y así realizar gastos, débitos e inclusive retiros con estas tarjetas clonadas. Para evitar que esta conducta se siga practicando dentro del país, el Estado realizo una campaña mediante la cual se ponía en sobre aviso a los ciudadanos los cuales realizan compras con sus tarjetas tanto de crédito como de débito en la que se hacía alusión que nunca despeguen la vista de sus tarjetas al momento de pagar, y así evitaban que estas fueran clonadas.

4.9.9. Carding

Una modalidad de ciberdelito existente y que aún se mantiene latente en la actualidad es el Carding, este consiste en utilizar un número de tarjeta de crédito existe y a través de este realizar compras en línea, dejando al usuario de esta tarjeta con una deuda que tendrá que cancelar en el momento de su fecha de corte, este tipo de delito es la secuela del phishing, pues una vez que el infractor obtiene los datos de la víctima es cuando procede a realizar las compras electrónicas sin dejar opción a la víctima de cancelar dichas transacciones.

4.10. La responsabilidad bancaria frente a los delitos informáticos

Según Villegas, en cuanto a la responsabilidad nos encontramos que “la imputación de una sanción a una conducta antijurídica que provoca perjuicios, es decir es la consecuencia (sanción) que la ley establece con motivo de una actuación humana voluntaria violatoria de la norma jurídica (sea la norma general o la norma particular) generadora de un perjuicio a otra persona”.

En este caso en concreto para la existencia de la responsabilidad y la imputación de una conducta deberá tener como base principalmente que esta responsabilidad sea siempre y cuando emanada por la banca o la institución financiera, nos encontramos principalmente con

el tema de que la banca pasa a ser una persona jurídica, misma que será sancionada en caso de cometimiento de una infracción con las penas establecidas para las personas jurídicas.

Las Instituciones Financieras dentro del país mantienen no solamente estatutos los cuales regulan su participación; sino que al momento de mantener el patrimonio de sus socios se convierte en aquel que se encargara de tutelar estos bienes u activos, tenemos principalmente el principio de confianza entre el banco y el usuario del mismo, nos encontramos con que aquellos que proceden a confiar en una institución financiera a fin de que resguarden sus bienes no deben responder por las afectaciones generadas por la insuficiencia en cuanto a medidas de seguridad por su banco de confianza.

La determinación de la culpa se establece según las reglas del Código Civil, diferenciando entre culpa contractual y extracontractual; originándose la primera en el caso que nos ocupa en los daños ocasionados por los bancos a sus clientes por el elemento contractual que los une, es decir cuando entre las dos partes banco – cliente se ha suscrito un contrato por el cual el primero oferta al segundo servicios de banca en línea; mientras que la segunda se origina por los daños sufridos sin que medie una relación contractual, por delitos o cuasidelitos, lo cual se origina ante la inexistencia de una relación previamente convenida como es el caso de los usuarios de la banca que sufren un daño sin ser clientes de ésta. Por ende, al existir un contrato que los vincula a sus clientes o socios la banca se encuentra en la obligación no solo civil sino también moral de proteger los activos de sus socios.

Los bancos son responsables ante sus clientes por los contratos que celebran con ellos, por lo que responden por la inejecución o defectuosa ejecución de las operaciones a las que se compromete; pero también es responsable ante sus usuarios por los actos efectuados por sus dependientes, pues principalmente al tratarse de sus operadores o trabajadores es de entender

que si es su deseo efectuar actividades ilícitas aprovechándose de su condición la institución financiera deberá trabajar en impedir que esto suceda.

En cuanto a la responsabilidad penal existente para la banca debemos recordar que esta al tratarse de una persona jurídica como lo es una banca se someten principalmente a la existencia de la responsabilidad y las sanciones que se encuentran establecidas en el Art. 71 del Código Orgánico Integral Penal, debemos tomar en consideración varios aspectos, el primero de ellos que se deberá demostrar la participación de una manera directa de la banca en el tipo penal, y no que se encuentre en calidad de una víctima; por ejemplo, en el caso de que una institución financiera procediera a comercializar a través de su gerente general, es decir aprobado por el encargado de la misma, la información bancaria de sus usuarios y esta llegara a conocimiento de un tercero que efectuaría un mal uso de esto, entonces la institución tiene la responsabilidad, pues existe un consintiente o la intención de ejecutar el daño, caso distinto seria si por ejemplo, uno de los trabajadores valiéndose de su puesto y en base al acceso que tiene proceda a comercializar la información de los usuarios, con ello pese a salir la información desde la institución, en realidad esta no conocía de manera directa lo que se estaba cometiendo, por lo que se puede alegar que no tiene ningún tipo de responsabilidad en dicho caso.

4.11. Medidas adoptadas por el sector financiero en ciberseguridad.

Dentro del presente trabajo de integración curricular uno de los pilares más importantes es el analizar las medidas adoptadas por las instituciones financieras en cuanto al manejo de sus plataformas virtuales y que medidas adoptan para poder dar a conocer su cumplimento y compromiso con la ciberseguridad de sus usuarios, estas medidas por cuanto son tomadas dentro de una institución financiera no son del todo abarcadas con amplitud ni expuestas abiertamente precisamente por el recelo existente en cuando a sus datos; aun con

ello de la revisión de las Memorias de Sostenibilidad de múltiples instituciones financieras podemos encontrar lo siguiente:

4.11.1. Banco de Guayaquil

El banco de Guayaquil publico dentro de sus memorias de sostenibilidad del año 2022 (que es la última de la cual se mantiene registro) los diferentes problemas que han tenido a lo largo de dicho periodo de operaciones; destacan tres vulnerabilidades importantes o tres problemas sobre los cuales han tenido que tomar medidas de prevención, la primera de ellas se trata del bloqueo de los canales remotos y digitales, dentro de estos se destacan la banca móvil de dicho banco así como también los diferentes cajeros automáticos a nivel nacional; su segundo problema más grave consiste en el robo de los datos de clientes, esto siendo contrarrestado con el control de los movimientos de las diferentes cuentas y control en cuanto a las transacciones, enviando diversos mensajes de confirmación a los números telefónicos de estos usuarios, finalmente destacan la suplantación de identidad de los clientes y los colaboradores (phishing)

El banco de Guayaquil destaca que "se ejecutan anualmente pruebas de phishing/ransomware a todos los colaboradores para poner a pruebas sus conocimientos en detecciones de anomalías y el proceso a seguir para reportar adecuadamente estos casos. Gracias a las medidas implementadas, se pudieron detener en un 73% posibles fugas de información personal de clientes"

Estas pruebas realizadas buscan en si analizar las diferentes anomalías que recibe no solo la institución financiera sino que además también busca proteger a sus usuarios ante el posible ataque a sus plataformas virtuales; finalmente el banco de Guayaquil implemento "la Oficina de Gobierno de Información y Analítica (OGA), cuyo propósito es facilitar el correcto gobierno de la información e incentivar las capacidades analíticas en toda la

institución, promoviendo así una cultura impulsada por datos.” Siendo esta la encargada de “la administración del conjunto de políticas, procesos y controles implementados para asegurar que la información de los clientes tenga una buena calidad y una estructura adecuada para responder a sus necesidades” con esa oficina de gobierno lo que se busca es mantener de manera adecuada la información de los clientes de la institución y sobre todo se busca evitar que estos sufran alguna vulneración a su información personal y sobre todo que estos sufran una afectación a su patrimonio que se encuentra en manos de dicha institución.

4.11.2. Banco del Pacifico

El banco del Pacifico en sus memorias de sostenibilidad se plantea tres objetivos claros para el tema de la ciberseguridad y para reducir el riesgo tecnológico que pueden llegan a tener, nos encontramos principalmente con que buscara identificar las posibles amenazas que estos enfrenten, vulnerabilidades e inclusive las consecuencias de los mismos para así encontrarse preparados para la gestión en caso de un posible ciberataque; también potencia su forma de pensar en cuanto a la reducción de las pérdidas económicas que puedan llegar a generarse debido a un ciberataque ante sus sistemas y finalmente como objetivo buscara el mejorar sus tecnologías de la información hasta el punto que estas sean confiables, estables y que sean disponibles a nivel no solo nacional sino que también lleguen hasta el nivel internacional; de esa manera esta institución bancaria hace el frente y gestiona sus tecnologías para que sus usuarios tengan la confianza y seguridad de que no sufrirán ningún tipo de ciberataque a su información.

4.11.3. Banco de Loja

El banco de Loja es una de las instituciones financieras más importantes de toda la región sur del país, se caracteriza por tener un gran número de socios y personas afiliadas dentro de sus instituciones, como tal el banco de Loja en sus Formas de contrarrestar los ataques de ciberseguridad nos encontramos con las siguientes propuestas tomadas en consideración:

-Capacitación y concienciación en ciberseguridad

Dentro de los aspectos que el Banco de Loja ha tomado en consideración para poder garantizar la ciberseguridad de sus usuarios es el desarrollar programas de capacitación hacia los colaboradores del mismo, en el cual se los expone, capacita y sobre todo educa dentro del ámbito de la ciberseguridad para con ello lograr evitar cualquier tipo de ataque que pueda generarse, las capacitaciones las realizan a sus trabajadores, pues ellos pueden llegar a ser víctimas del phishing, con ello garantizan que la información o la afectación no venga de manera directa por parte de uno de los trabajadores de la misma Institución financiera.

-Ejercicio de red Team

Es una política implementada por el Banco de Loja, ejecutada por dos veces al año y que busca la simulación de un ataque dirigido a la institución financiera, evaluando las posibilidades de poder acceder a los sistemas informáticos de la Institución, con la finalidad de poder encontrar aquellos puntos débiles de los sistemas, se ejecutan mediante el uso de una metodología explicada de manera gráfica en las memorias de sostenibilidad de la siguiente manera:

- **Hackeo ético**

El Banco de Loja con el fin de prevenir el impacto económico, operativo y de reputación que puede tener este tipo de ciberataques, contrató una empresa certificada a nivel Internacional para realizar un hackeo ético, el resultado les permitió fortalecer y mejorar la seguridad de la infraestructura tecnológica de la Institución tanto interna como externa,

aplicando planes de mejora en los procesos de seguridad del Banco, siendo esta medida una de las mejores tomadas para poder ejecutar los diferentes procesos que esta tenga de por medio.

-Centro de Operaciones de Ciberseguridad (CyberSOC)

El CyberSOC es una herramienta tecnológica que permite proteger de forma proactiva y permanente los datos y sistemas informáticos ante las diferentes amenazas presentes en la red, está operado por profesionales altamente capacitados en el área de seguridad informática y de infraestructura de TI. Los recursos, procesos y aplicaciones del CyberSOC están operativos 24/7, para proteger al Banco de Loja de eventuales riesgos que puedan afectar sus operaciones, enfocándose principalmente en la detección de actividades sospechosas en tiempo real, como solicitudes falsas de conexión, intentos de intrusión o fuga de información. Es sin lugar a dudas aquello que ha permitido que dicha Institución financiera no presente mayor problema dentro de sus plataformas digitales y con ello además protege al usuario de las mismas.

4.12. Manejo de indicios y/o evidencia digital

De conformidad a los diferentes instructivos que maneja la Fiscalía General del Estado mediante el Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses se elaboró un Instructivo el cual anuncia a los peritos y personal que trabaja con la evidencia digital en cuanto a la manera en la cual esta debe ser manejada para poder efectuar los informes periciales que consideren pertinentes o que sean procedentes dependiendo de cada caso en concreto, para el tratamiento de la evidencia digital se debe tomar en cuenta estos parámetros:

"Fijación Digital de los dispositivos y equipos informáticos en funcionamiento:

La fijación digital se fundamenta en tres tomas fotográficas:

a) Estado inicial del equipo, componentes y conexiones (accesorios externos del equipo).

b) Plaquetas de identificaciones técnicas (número de serie y modelo).

c) Fijación del escritorio (ubicación de los íconos instalados por programas).”

Como un primer acercamiento al momento de verificar la existencia de un equipo informático el cual mantenga evidencia digital se debe proceder con las tomas fotográficas del equipo en todos sus etapas, partiendo desde el estado inicial en aspecto físico como también el número de identificación y los programas instalados, esto se realiza con la finalidad de que se garantice que el equipo que se encuentra bajo objeto de pericia sea el adecuado y no se lo suplante por otro equipo de similares características.

i. Captura de la Memoria RAM.

a) Acoplamiento físico por un interfaz nuevo (USB, disco externo, cd, DVD, etc.) proporcionado por el Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses.

b) Volcado (adquisición) de la información capturada al medio externo para su conservación y preservación.

c) Apagar el dispositivo y/o equipo informático.

d) Entrega del medio de almacenamiento, al Centro de Acopio e inicio de cadena de custodia.

En este caso nos encontramos con la situación de una transcripción o traspaso a un interfaz nuevo para efectuar el traspaso de la documentación y de los archivos digitales que tenga algún dispositivo electrónico, nos encontraos con el hecho principal que el medio externo debe ser proporcionado por el mismo Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, además que una vez se complete el volcado se procederá a apagar el dispositivo y entregar en el centro de acopio para por fin dar

por iniciada la cadena de custodia respectiva para someter la información digital a las pericias del caso.

b. Fijación Digital de los dispositivos y equipos informáticos que se encuentren apagados:

a) Identificación del dispositivo y/o equipo informático, componentes y conexiones (accesorios externos del equipo).

b) Plaquetas de identificaciones técnicas (número de serie y modelo).

c) Fijación del indicio en el lugar de los hechos e inicio de cadena de custodia.

Para el caso de la existencia de un dispositivo electrónico el cual se encuentre apagado a la hora de la aprehensión es importante que se comience con la apertura de la cadena de custodia, todo ello para poder encenderlo y extraer la información requerida sin que se pueda llegar a alegar vulneración a algún derecho de la persona investigada. Este es el proceso adecuado y la forma mediante la cual se debe proceder con la extracción de la información digital y pericias a desarrollarse en los diferentes equipos electrónicos.

4.11. Constitución de la República del Ecuador (2008)

La Constitución de la República del Ecuador es la norma más importante que rige el sistema jurídico, así como también los derechos y las obligaciones tanto de los ciudadanos como también del Estado para con sus habitantes, con ello al ser la norma más importante a nivel nacional es de entender que regule casi todas las relaciones existentes dentro de un determinado estado; así dentro de nuestro ámbito de estudio en el control y sanción de los ciberdelitos podemos destacar puntualmente ciertos artículos que trabajaran con otras normativas para garantizar los derechos de los ciudadanos ecuatorianos.

“Artículo 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características. La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.” (Constitución de la República del Ecuador, 2008)

Como uno de los derechos constitucionales más importantes encontramos la libre disposición de los bienes además del recibir servicios de óptima calidad los cuales elegiremos con libertad, teniendo acceso a información precisa y nada engañosa en las características del producto, es lo que se conoce en el mundo del derecho como la protección del consumidor, en ese sentido es derecho de los ciudadanos que cuando se nos oferte un producto o servicio este deberá cumplir con múltiples características o con ciertos lineamientos necesarios para que estos sean óptimos y no tengan ningún peligro de ser usados, esto incluye la protección de los datos personales para aquellas empresas o instituciones las cuales manejan nuestros datos.

“Artículo 53.- Las empresas, instituciones y organismos que presten servicios públicos deberán incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras, y poner en práctica sistemas de atención y reparación. El Estado responderá civilmente por los daños y perjuicios causados a las personas por negligencia y descuido en la atención de los servicios públicos que estén a su cargo, y por la carencia de servicios que hayan sido pagados.” (Constitución de la República del Ecuador, 2008)

Bajo este artículo constitucional ordena a las empresas tanto privadas como públicas el incorporar una forma para poder satisfacer las necesidades de los usuarios y además de practicar de manera integral la atención a los mismos, esto en todo lo relacionado en la prestación de sus servicios, con ello las empresas están obligadas a responder por todas sus actuaciones que se generen desde su toma de decisiones hasta el tomar acciones en caso de que sean requeridas para salvaguardar ya sea la información de sus usuarios o bien los datos que estas manejan, en tal sentido, es de vital importancia que tanto el Estado como la empresa pública o privada trabajen en conjunto y así garantizar la seguridad de los usuarios y también la protección de sus datos personales.

4.12. Reunión Global sobre la Sociedad de la Información de Ginebra (CMSI) y Convenio de Budapest.

El convenio de Budapest es uno de los primeros creados con la finalidad de poder delimitar a que se refiere todo el tema de ciberdelincuencia así como también los procedimientos los cuales se deberán tomar en el caso de que exista el cometimiento de uno de ellos, firmado en la ciudad de Budapest, el 23 de noviembre del año 2001, establece principalmente cual será el procedimiento de los Estados firmantes para dar investigación a los ciberdelitos todo ello amparados en el tipo penal del cual se tratase, establece la responsabilidad jurídica de las personas tanto naturales como jurídicas, además de ello delimita el procedimiento mediante el cual se tomaran medidas para trabajar con estos delitos.

Además de los datos ya mencionados el Convenio de Budapest establece que los estados firmantes y ratificantes del mismo convenio deberán adoptar las medidas legislativas necesarias para poder conservar las diferentes evidencias y respaldos necesarios a la hora de la sanción de este tipo de delitos, confiere la necesidad de que se opten por formas en las

cuales se proteja esta información con el respectivo respeto a las formalidades de cada estado, así mismo confiere a los Estados firmantes la delegación de adoptar medidas en las cuales las autoridades jurisdiccionales puedan acceder de manera rápida y eficiente a cualquier fuente de datos existente, sin que su requerimiento carezca de validez jurídica, también el proceder con el confisque de los datos en donde sea que se encuentren almacenados, con ello le brinda a todos sus países firmantes las herramientas a fin de que se pueda investigar estas causas de la manera más acertada posible y evitar sobre todo la impunidad de los presuntos infractores.

4.13. Normas ISO/IEC 27037:2012.

Las normativas ISO/IEC son un conjunto de estándares internacionales los cuales fueron creados con la finalidad de que las empresas mantengan una línea homogénea en cuanto a la gestión, prestación de servicios y desarrollo de productos dentro de una determinada industria, teniendo sus orígenes en el año de 1946; las siglas ISO significan International Organization for Standarization, y cada una de ellas abarca un aspecto puntual en los procesos que se deben seguir para determinadas acciones dentro de las empresas, las normas ISO/IEC 27037:2012 proporciona orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio. Se orienta a su uso en investigaciones forenses digitales, destinadas al esclarecimiento de hechos en los que interviene de alguna forma un recurso electrónico o digital.

Dentro de estas normativas nos encontramos con la preservación digital de los dispositivos electrónicos tales como lo son medios de almacenamiento digitales utilizados en ordenadores tales como discos duros, discos flexibles, discos ópticos y magneto ópticos, dispositivos de datos con funciones similares; teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria, sistemas

de navegación móvil, cámaras digitales y de video (incluyendo CCTV), ordenadores de uso generalizado conectados a redes, redes basadas en protocolos TCP / IP y otros dispositivos con funciones similares a las anteriores; con ello las normativas ISO buscan proteger los dispositivos y más importante aún la información que estos contienen o almacenan en su interior, pues en base a ellos se inician las investigaciones respectivas en los casos necesarios.

Así mismo estas normativas claramente buscan el proporcionar orientación sobre el manejo de la evidencia digital, siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación a entornos jurisdiccionales (juicios y arbitrajes) además de lograr cubrir toda una gama de tipos de dispositivo y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable. Por lo que al ser estándares de categoría internacional su aplicación nos facilita como sistema jurídico el preservar de una mejor manera la información que logremos recabar de todas las investigaciones de ciberdelitos que lleguen a nuestro conocimiento.

4.14. Código Orgánico Integral Penal (2014).

El código Orgánico Integral Penal del año 2014 cuya última reforma se encuentra en el año 2024 ha conferido a todos los ecuatorianos una normativa legal que facilita la sanción y tipifica las conductas que sean penalmente relevantes, con ello se puede llegar a determinar que gracias al Código Orgánico Integral Penal se buscan las sanciones a aquellas personas que inflijan la normativa y a su vez buscar una reparación integral a las víctimas por la comisión de estos delitos, principalmente en el tema de los ciberdelitos contamos con un apartado muy amplio que no solamente tipifica las sanciones y las conductas penalmente relevantes sino que además confiere términos los cuales son importantes tratar para poder entender a ciencia cierta cuando se trata de un ciberdelito, al ser una cantidad elevada de

conductas que pueden ser cometidas no se detallan todas, sin embargo trabajaremos con las más relevantes para esta investigación.

"Artículo 190.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas encriptados, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes." (Código Orgánico Integral Penal, 2014)

Nos encontramos con uno de los delitos que más pueden llegar a involucrar a los sistemas informáticos siendo este el fraude informático, directamente relacionado con las redes y telecomunicación es un verbo rector el cual sanciona a las personas que de una manera fraudulenta ingresen a los sistemas informáticos y se apropie de un bien que no le pertenece gracias a esta acción, con ello deja claramente delimitado la persona y la conducta de la cual se trata esta investigación, además al tratarse de un delito cometido a través de los medios tecnológicos es de trascendental importancia que este sea tratado con la brevedad del caso y bajo los correctos estándares internacionales de conservación de la información.

"Artículo 231.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un tercero, será sancionada con

pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona."

Dentro del Sistema Financiero Nacional existen un sin número de programas informáticos que ayudan para la generación de las diferentes estructuras que son exigidas para el funcionamiento a su vez estas se realizan de manera exhausta por cuanto pueden ser jaqueadas, esta acción del hackeo genera las afectaciones a los usuarios de los diversos sistemas informáticos, es de entender que estos sistemas de bancas electrónicas recopilan una gran cantidad de datos de sus usuarios mismos que a su vez mantienen sus activos dentro de las instituciones bancarias lo que puede ser información vulnerable y que debe ser guardada con las garantías de ley para evitar así su mal uso, además de aquello es de entender que esta información es delicada en ciertos aspectos por lo que su manipulación puede devengar en un sinfín de problemas tanto para el usuario como para la persona que tiene dicha información. .

"Artículo 233.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad."

Existe en el Ecuador información clasificada como confidencial que por su importancia no puede ser divulgada, y que en muchos de los casos se ha transferido a personas para que hagan uso doloso de la misma, es de suma importancia que las personas que divulguen esta información considerada como confidencial tengan una sanción que vaya de acorde al tipo de información que se divulgue, por lo que deberá trabajar de manera directa el Estado con el apoyo de los órganos jurisdiccionales para proceder a proteger estos datos de suma importancia, este verbo rector abarca la destrucción de información de suma importancia siempre y cuando estos reposen en archivos digitales o medios telemáticos, .

4.15. Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales confiere a los ciudadanos la protección inequívoca en cuanto a lo referente a sus datos que reposen en diferentes archivos, pudiendo estos ser archivos físicos o digitales, con ello está más que claro que la protección por parte del Estado esta brindada, pero esta debe ser reforzada, principalmente destacamos un artículo de esta normativa que destaca lo siguiente:

"Art. 38.- Medidas de seguridad en el ámbito del sector público. - El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales."

La normativa confiere al sector gubernamental la obligación de mantener medidas de seguridad con el tema del tratamiento de los datos personales ante la existencia de cualquier amenazada, frecuentemente en los últimos años se han filtrado múltiples amenazas por parte de los llamados hackers que han accedido a los sistemas informáticos y que mantienen los

datos de las personas como una herramienta que puede ser ocupada para posteriormente cometer ilícitos, es importante tomar en consideración que estas actuaciones al deber ser tomadas por los gobiernos locales y el Estado como máximo órgano gubernamental debe apoyarse en la medida de lo posible para ejecutar las acciones que por ley creyeran convenientes, no está por mas indicar que en caso de que se sufra la vulneración de la información en la medida de lo posible, es de igual manera responsable la Institución Financiera si desde sus archivos se ha desprendido la información, pudiendo reclamar la presunta víctima una reparación de acorde a los daños causados.

4.16. Resoluciones Interinstitucionales entre la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros

Ante las diversas denuncias presentados dentro de varios años ante la Fiscalia, se buscó realizar una resolución en conjunto con la Superintendencia de Bancos y Seguros, con la finalidad de en cierto sentido ejercer presión en las diferentes instituciones bancarias a nivel nacional por el aumento de las denuncias por ciberdelitos, ya que los perjuicios ocasionados a los usuarios de la banca llegaron hasta la cantidad de tres millones y medio de dólares de los Estados Unidos de América, por lo que amparados en la Ley de Defensa al Consumidor y la Ley de Comercio Electrónico se emitieron dos resoluciones las cuales explicaremos su parte resolutiva de la siguiente manera:

4.16.1. Resolución Interinstitucional Nro. 001-FGE-SBS-2011

Dentro de esta resolución que constituye la primera dentro del ámbito de la ciberseguridad encontramos las siguientes letras las cuales detallaremos a continuación:

“a) Se dispuso que las instituciones del sistema financiero inicien correctivos para impedir el cometimiento tanto del delito de fraude informático como de los delitos relacionados con lavado de activos”

Con este numeral se garantiza por parte de la Fiscalía y la Superintendencia que los bancos procedan a tomar medidas necesarias a fin de evitar que sus clientes caigan dentro del delito de fraude informático, además de ello buscan el tema de reducir el tema del lavado de activos a través del uso de los medios informáticos, en tal sentido el estado ha delegado la función a las instituciones financieras del control de los diferentes transacciones y medios electrónicos.

"b) Se concluyó que la banca era responsable directa e indirectamente por los fraudes informáticos sufridos por sus clientes."

Este punto es bastante importante en cuanto a la gestión ocasionada por parte de la Fiscalía en cooperación con la Superintendencia de Bancos y Seguros, en tal sentido ha atribuido a los bancos e instituciones del sector financiero la responsabilidad por los fraudes informáticos que lleguen a sufrir los clientes de dichas instituciones, ante ello deja en tela de duda si esto se debió por el filtrar la información confidencial de los usuarios de los diferentes medios telemáticos o si esto se debió a un ataque a los sistemas de las instituciones financieras por lo que su responsabilidad podría llegar a entenderse como una de carácter solidaria, mas no en calidad de autores de los ilícitos, aun con ello para esto opera el principio de confianza que deposita el usuario o cliente ante la institución para que esta mantenga su patrimonio, por lo que la responsabilidad es exclusiva de la banca.

"c) Se dispuso que las instituciones del sistema financiero "reconozcan" a sus clientes perjudicados por delitos de fraude bancario entre el período comprendido del 1ro de enero del 2010 hasta el 21 de marzo del 2011, según el monto reclamado."

Principalmente mediante esta resolución al dar origen debido a un problema social en el cual existieron varias personas afectadas a causa de los delitos informáticos se ordena la reparación integral de las mismas, todo esto por cuanto al no tener ningún tipo de

responsabilidad en las actuaciones erradas ya sea de la institución o en sus funcionarios, no se trataba de un daño que pueda ser previsible y por consiguiente debían ser reparados integralmente con los montos los cuales se les fueron arrebatados.

Para ello la misma resolución emite diferentes formas en las cuales se da esta reparación relacionadas exclusivamente a los montos que les fueron sustraídos en base a la siguiente situación:

"los clientes que habían sufrido pérdidas de un dólar hasta dos mil dólares se les restituiría el cien por ciento; a los clientes que habían sufrido pérdidas de dos mil un dólar hasta diez mil dólares se les restituiría el ochenta por ciento; y a los clientes que habían sufrido pérdidas de más de diez mil dólares se le restituiría el sesenta por ciento"

Estas pérdidas son restituidas en base a la proporcionalidad del daño efectuado al bien jurídico protegido que dentro de este caso corresponde principalmente al patrimonio o a la propiedad, pues es de esa manera en la que esta resolución así lo habría dispuesto, con ello la Superentendía confiere a los usuarios las herramientas necesarias para poder conseguir y lograr una reparación integral de acorde a los daños que sufrieron y de conformidad a lo que establecía la normativa de ese tiempo.

"d) Se dejó a salvo el derecho de las personas que no querían aceptar los montos señalados para seguir las acciones correspondientes."

Principalmente al tratarse de un tema en el cual existe de por medio una cantidad monetaria y por cuanto es prioridad del estado el garantizar todas las formas de la propiedad, deja abierta la puerta para que las personas que no aceptaren esta disposición puedan reclamar ante la autoridad competente la restitución total del daño efectuado y la repara ración integral a la víctima, además de interponer, en este caso por tratarse de personas

jurídicas las naciones administrativas que sean procedentes, esto con la finalidad de poder hacer efectivos sus derechos constitucionales y legales.

Esos fueron los hechos principales que se toparon dentro de la resolución Nro. 001-FGE-SBS-2011; principalmente trabajaría con estos mecanismos adoptados por parte de la banca para poder garantizar la reparación integral de la víctima y reparación de los daños efectuados, esta reparación por parte de la banca por tratarse de una responsable solidaria.

4.16.2. Resolución Interinstitucional Nro. 002-FGE-SBS-2011

Emitida como una ampliación a la resolución antes descrita esta resolución que le sigue manifiesta principalmente lo siguiente:

"a) Que para viabilizar el reintegro de los valores determinados en la resolución 001–FGE – SBS – 2011 se requería que las personas beneficiadas por ésta firmen un acta de conformidad con las respectivas entidades bancarias mediante la que se liberaba al banco pagador y a sus funcionarios de cualquier otro nuevo reclamo sobre los hechos materia del reclamo originario"

Principalmente y lo más destacable por parte de esta resolución es que menciona el deber objetivo de firmas un acta a fin de que esta sea debidamente registrada para evitar futuros inconvenientes por los mismos hechos que se inician la investigación; siendo este un alcance a la figura conferida en dicha resolución.

4.16.3. Resolución Nro. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.

Resolución dictaminada por parte de la Superintendencia de la Economía Popular y Solidaria en el año del 2022, regula todos los aspectos concernientes a la seguridad de la información en las entidades que comprenden el sector financiero, popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria, para ello la normativa ha previsto que en su parte pertinente trabaja referente a la forma en la cual se buscara proteger

la seguridad de los usuarios de dichas instituciones, manifestando que cada una de las instituciones que lo conforman sean con:

"Art. 5.- Régimen General. - Conforman el régimen general de seguridad de la información:

a) El Consejo de Administración o el Directorio, según corresponda;

b) El Comité de Seguridad de la Información (CSI)

c) El Gerente General o Representante Legal;

d) La Unidad o Departamento de Seguridad de la Información;

e) El Oficial de Seguridad de la Información (OSI)"

Dentro del régimen general aplicable a las Cooperativas e Instituciones que conforman la Economía Popular y Solidaria se crean determinados departamentos los cuales se encuentran el Comité de Seguridad de la Información el cual se encargara de las maneras en las cuales se trabajaran los datos de los usuarios y socios, además de tener de igual manera un departamento encargado de la seguridad de la Información, el cual realizara el seguimiento respectivo a los datos que confieren los usuarios a las instituciones financieras, aun con ello, estos datos y manejo se desarrolla únicamente en el ámbito de los datos físicos, no realiza un control de los datos de manera digital, así que los medios telemáticos en la actualidad aun no son protegidos por parte de la Superintendencia.

4.17. Derecho comparado.

La situación actual del Ecuador en cuanto a la investigación y persecución de los ciberdelitos, así como también el estudio de este tipo de actividades es en cierto sentido deficiente, no existe una forma clara mediante la cual el Ecuador pueda trabajar de manera oportuna en la intervención, prevención y sanción de los delitos cometidos dentro de este parámetro, es por ello que se han analizado los siguientes países en los cuales se ha tenido que tipificar dichas conductas delictivas por cuanto las mismas violentan los derechos de los socios y usuarios y de la ciudadanía.

4.17.1. Código Penal Federal (México)

La legislación mexicana siendo una de las más golpeadas y afectadas por el narcotráfico y siendo de las que más han contenido influencia de las mafias, ha provocado que su sistema penal se encuentre bien reforzado para poder avanzar con los diferentes problemas que puede devengarse y la protección de los sistemas informáticos no es la excepción, dentro del caso de la legislación mexicana nos encontramos principalmente con que estos artículos:

"Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública" (Codigo Penal Federal, 2009)

El derecho penal mexicano sanciona a cabalidad a aquellos que se infiltran en las bases de datos de las instituciones pero además de ello a aquellos que provoquen la destrucción de los mismos en base a los diferentes recursos de ellos, con esto el derecho penal mexicano protege a las instituciones y les garantiza la persecución de los ciberdelitos cometidos con las personas que se infiltran a las redes.

4.17.2. Legislación Española

4.17.2.1. Código Penal

El código penal español nos otorga un amplio catálogo de ciberdelitos los cuales cuentan con su respectiva sanción en cuanto se han cometido, principalmente para nuestro

trabajo de integración curricular, por cuanto se trata de buscar las vulnerabilidades de los sistemas informáticos de las diferentes instituciones del sector económico popular y solidario se adecua los siguientes artículos:

Art. 249: "1. También se consideran reos de estafa y serán castigados con la **pena de prisión de seis meses a tres años**:

a) Los que, con ánimo de lucro, **obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial** en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo." (Codigo Penal, 2009)

El mencionado artículo reconoce como tal el actuar de una persona ajena al sistema informático y por ende reconoce que este se encuentra vulnerando su seguridad, aun con ello, dentro del almanaque de delitos informáticos de la legislación española no encontramos

ningún artículo que mencione cómo será la sanción aplicable para el caso de que una persona vulnere los sistemas informáticos.

Art. 264: "1. El que, por cualquier medio, sin autorización y de manera grave **borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años**.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero."

Dentro de dicho artículo la legislación española nuevamente menciona a los infractores en este caso como actores directos de la afectación a los sistemas informáticos provocando su daño y afectación a los sistemas, lo que deslinda que estos serán sancionados con una pena bastante ligera pero la multa aplicable será proporcional a los daños efectuados, situación que en el Ecuador si bien se debe garantizar el principio de proporcionalidad este no afecta de manera directa a la multa impuesta por ello.

4.17.2.1. Código de Derecho de la Ciberseguridad

En España, se cuenta con un Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio y el velar por la mencionada ciberseguridad, dentro de los diferentes aspectos que prevé esta codificación nos encontramos con varias normativas de protección esenciales en el aspecto de la ciberseguridad como son la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, misma que en su Art. 39 manifiesta lo siguiente:

"**Artículo 39.** Comunicación de una violación de la seguridad de los datos personales al interesado. **1.** Cuando existan indicios de que una violación de la seguridad de los datos personales supondría un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará al interesado, sin dilación indebida, la violación de la seguridad de los datos personales"

Dentro del presente caso nos encontramos efectivamente con un aspecto fundamental en cuanto a los datos personales y lo que es la acción efectiva de los mismos, ante ello nos podemos percatar que la primera persona en enterarse de la vulneración de sus datos personales es el dueño de dichos datos, con lo cual es importante actuar de manera directa por parte del Estado Español, este tratamiento e iniciativa puede llegar a ser efectuada de manera

oportuna por parte de las instituciones financieras en las cuales se busca velar e intentar prevenir la existencia de fugas de capital, situación que no sucede en el Ecuador.

4.17.3. Reglamento a la Seguridad Cibernética y de la Información (República Dominicana)

La legislación de Republica dominicana a través de sus diferentes instituciones ha emitido un Reglamento a partir de la Junta Monetaria el cual concibe múltiples aspectos en cuanto a la ciberseguridad dentro de la información y sobre todo en el sector económico financiero del país, de dicha legislación podemos encontrar los siguientes puntos a considerar:

"Artículo 3. Ámbito de Aplicación. Las disposiciones establecidas en este Reglamento son de aplicación para las entidades que se identifican a continuación: **a)** Bancos Múltiples; **b)** Bancos de Ahorro y Crédito; **c)** Corporaciones de Crédito; **d)** Asociaciones de Ahorros y Préstamos; **e)** Entidades Públicas de Intermediación Financiera; **e)** Administradores de Sistemas de Pago y Liquidación de Valores; **f)** Participantes del SIPARD autorizados por la Junta Monetaria; y, **f)** Cualquier otro tipo de entidad del SIPARD, que la Junta Monetaria autorice en el futuro." (Congreso Nacional, 2007)

Como se detalla dentro del ámbito de aplicación de dicho reglamento este trabajara de manera exclusiva y sobre todo en cuanto a los bancos, cooperativas de ahorro, en si dentro de todos los sectores económico financieros a nivel nacional, con ello la ley que se encuentra establecida permite a los usuarios trabajar de manera pormenorizada con los sectores financieros lo que les compromete independientemente de los servicios que estos presten, además de ello estos sectores son de vital ayuda e importancia por cuanto con ello se busca respaldar el accionar de los diferentes sectores financieros y económicos a nivel nacional.

Artículo 9. "Responsabilidades del Comité Funcional de Seguridad Cibernética y de la Información. El comité funcional de seguridad cibernética y de la información asumirá, de manera enunciativa, pero no limitativa, las responsabilidades siguientes: **a)** Diseñar los lineamientos funcionales de Seguridad Cibernética y de la Información, y el mantenimiento del Programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad, determinados por el consejo u órgano societario equivalente; **b)** Someter al consejo u órgano societario competente, para su aprobación, las políticas del Programa de Seguridad Cibernética y de la Información; **c)** Evaluar la

efectividad del Programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad; **d)** Ratificar las decisiones de tratamiento de riesgo, en coordinación con las áreas pertinentes de negocio, previamente presentadas por el Oficial de Seguridad Cibernética y de la Información; y, **e)** Comunicar al consejo u órgano societario competente, los resultados de sus valoraciones sobre los aspectos de Seguridad Cibernética y de la Información." (Congreso Nacional, 2007)

Dentro de dicho reglamento establece la creación de un comité especializado y funcional en cuanto a la seguridad cibernética y de la información, este tipo de seguridad será en su principal forma de trabajo una forma mediante la cual se evalué, controle y actué de manera efectiva ante el posible ataque cibernético dentro de las instituciones, es por tal motivo que esta legislación, a comparación de la legislación ecuatoriana se sobrepone, pues si se cuenta con un mecanismo de operación inmediata para dar respuesta a las necesidades de las Instituciones tanto públicas como privadas, siendo respaldados por la ley.

Para mayor explicación de los puntos antes singularizado trabajaremos con el siguiente cuadro:

5. Metodología

Para el desarrollo y enfoque que se utilizó a lo largo de la investigación se enfoca en la metodología, primero guiándose con la utilización de los diferentes materiales que se emplearon para una mayor eficacia investigativa, seguido de la aplicación de diferentes métodos que facilitaron el desarrollo de la investigación, siendo que se emplearon los métodos como; método científico, método inductivo, método analítico, método exegético, método hermenéutico, método mayéutico, método comparativo, método estadístico. Al utilizar los diferentes métodos también se pudo determinar el enfoque de la investigación demostrado un enfoque mixto a lo largo del trabajo de integración curricular, demostrado con el refuerzo del tipo de investigación practicada. Finalmente para la conclusión de eficaces resultados se empleó el uso de técnicas donde se emplearon mecanismos como encuestas y entrevistas, realizadas a una población y muestra determinada como son; las encuestas aplicadas a treinta (30) profesionales del Derecho en libre ejercicio, mientras que en las entrevistas se realizaron de acuerdo al enfoque de la investigación y al fondo de la misma, un (1) tipo de entrevista las cuales serían aplicadas a tres (3) profesionales del derecho los cuales son especialistas en Derecho financiero y que además de ello laboran en relacion de dependencia con diferentes instituciones bancarias e instituciones de la economía popular y solidaria.

5.1. Materiales.

Los materiales utilizados para la realización del presente trabajo de integración curricular en relación a la bibliografía señalada, tenemos:

Diccionarios jurídicos, estudios realizados por diferentes universidades en países extranjeros, obras literarias en la rama jurídica, revistas jurídicas y de criminología de ámbito internacional, leyes de la legislación ecuatoriana, leyes de legislaciones extranjeras como

Perú, además de sentencias emitidas en Ecuador y noticias para el análisis de casos. Se empleó este recurso con la finalidad de que sirva para la redacción e interpretación personal del tema, mismas que se encuentran citadas dentro de mi trabajo investigativo.

Entre los diferentes materiales e insumos que facilitaron el desarrollo del presente trabajo son:

Computadora portátil, acceso a internet, teléfono celular y grabadora de la misma para las entrevistas, cuaderno para la toma de apuntes, impresiones y copias varías con el contenido del borrador del presente trabajo de integración curricular, etc.

5.2. Métodos.

Para el desarrollo del presente trabajo de integración curricular se aplicaron los siguientes métodos:

5.2.1. Método Científico.

Este método, que tiene la finalidad de obtener conocimientos desde el punto de vista científico, se utilizó en el presente trabajo con la finalidad de demostrar la problemática existente, recopilando una serie de textos jurídicos, doctrinarios y estudios científicos sobre la materia, mismos que sean citado y comparado con la legislación ecuatoriana, para verificar la realidad social.

5.2.2. Método Inductivo.

Se empleó el método inductivo, pues como lo menciona parte de lo particular a lo general, siendo aplicado cuando se describió la limitante existente en nuestra ley que conlleva en consecuencia derechos vulnerados de la ciudadanía.

5.2.3. Método Analítico.

Este método se utilizó con la finalidad de analizar y dar una opinión propia, con los diferentes criterios expuestos por los diferentes tratadistas o leyes, cabe mencionar que también se empleó al momento de analizar y comentar los diferentes criterios encontrados en las encuestas y entrevistas.

5.2.4. Método Exegético.

El método exegético se empleó al momento de analizar cada una de las normas jurídicas utilizadas para fundamentar la base legal, siendo estas, Constitución de la República del Ecuador, Código Organico Integral Penal, Ley Orgánica de Protección de Datos Personales con su respectivo Reglamento; Ley Orgánica de Defensa del Consumidor y las leyes internacionales aplicadas en el derecho comparado.

5.2.5. Método Hermenéutico.

La finalidad de este método es la interpretación de textos, por lo tanto, se utilizó con el fin de interpretar las leyes ecuatorianas y extranjeras para así poder determinar las diferentes vulneraciones existentes a los sistemas informáticos de las instituciones financieras asi como tambien la persecución de los delitos cometidos a estas.

5.2.6. Método Mayéutica.

Se utiliza para la recopilación de información a través de preguntas, en el caso del presente trabajo, se recopilo y utilizo este método a través del estudio de campo, en base a las respuestas obtenidas en las encuestas y entrevistas, que sirvieron para demostrar la problemática latente en la sociedad ecuatoriana.

5.2.7. Método Comparativo.

Bajo el enfoque del método comparativo que consiste en realizar comparaciones, se realizó la comparación entre la legislación ecuatoriana principalmente en base del Código

Organico Integral Penal y Ley Orgánica de Protección de Datos Personales con su reglamento con la norma internacional de Argentina, España, Uruguay y Republica Dominicana en base a los delitos informáticos o ciberdelitos, su forma de prevención y sanción.

5.2.8. Método Estadístico.

En este método se manejan los datos tanto cualitativo como cuantitativo de la investigación, por lo tanto, se lo utilizo al momento de obtener tanto los datos de las encuestas como de las entrevistas realizadas, referente a la información de las encuestas se representaron en gráficos y tablas, después de su respectiva tabulación; asi mismo se utilizó datos estadísticos concernientes a la actualidad que vive el pais en cuanto a los delitos informáticos y como estos se han tramitado.

5.3. Enfoque de la investigación.

El enfoque de la investigación que se realizó, es un enfoque mixto, pues se realizó una investigación tanto cualitativo y cuantitativo, ya que consta de estadística que se desarrolló gracias a las encuestas realizadas y la tabulación de la misma, por lo tanto, se realizó la investigación cuantitativa. Mientras que la investigación cualitativa, se desarrolló en base a las entrevistas, pues son datos relativos a cualidades, comentarios realizados en base a las preguntas realizadas. Por lo que, al aplicar tanto una investigación cuantitativa como cualitativa se convierte en un enfoque de investigación mixta.

5.4. Tipo de investigación.

El tipo de estudio en que se enfoca el trabajo de integración curricular es documental, pues se apoya en fuentes documentológicas, como la investigación bibliográfica basada en libros y de la investigación hemerográfica que se utilizó en las revistas, noticias, artículos y ensayos.

Cabe mencionar que el tipo de investigación también es de campo, pues se apoyó en información que viene de entrevistas, encuestas realizadas, además tomo en cuenta los estudios realizados por otras Universidades.

5.5. Población y muestra.

La población es un grupo de personas, mientras que la muestra es una serie de conocimientos dentro de la población a evaluar, por lo tanto, tanto la población como la muestra se enfoca en los Abogados del Libre ejercicio y las opiniones del tema de los fiscales y jueces.

Por ende, para una mayor comprensión de la problemática, se utiliza una población y muestra de 30 profesionales de derecho en libre ejercicio en base a las encuestas. Como también, entrevistas, donde se las realizó a tres individuos que se dedican al ejercicio de la profesión de la abogacía dentro de diferentes instituciones financieras.

5.6. Técnicas.

Encuesta: en la encuesta se plantea un cuestionario con una serie de preguntas objetivas, con la finalidad de obtener resultados, por lo tanto, para el correcto desarrollo de la investigación se aplicó una encuesta a treinta (30) profesionales del derecho en libre ejercicio, dicha encuesta constaba de cinco preguntas, donde se podía responder con un ‘‘Si’’ o un ‘‘No’’, además, de responder el ‘‘por qué’’ de su respuesta, para una mayor comprensión, a lo posterior se realizó la tabulación de los datos obtenidos.

Entrevistas: estas consisten en un dialogo entre el entrevistador y el entrevistado, por lo tanto, se realizó entrevistas, con cinco preguntas abiertas a tres personas, todas estas personas abogados los cuales dirigen el departamento jurídico de diferentes instituciones financieras.

6. Resultados.

6.1. – Resultados de las encuestas

Con el fin de poder realizar una correcta investigación, se llevó a cabo un trabajo en campo dentro del presente estudio jurídico y doctrinario, mediante el empleo de una encuesta a una muestra de treinta (30) abogados en libre ejercicio de la profesión, en la ciudad de Loja, mediante cinco preguntas cerradas relacionadas con el trabajo de investigación, arrojando los siguientes resultados con su respectivo análisis, mismos que se detallan a continuación:

Primera Pregunta:

¿Conoce usted la norma jurídica que regula los ciberdelitos y la información de los usuarios del sector financiero?

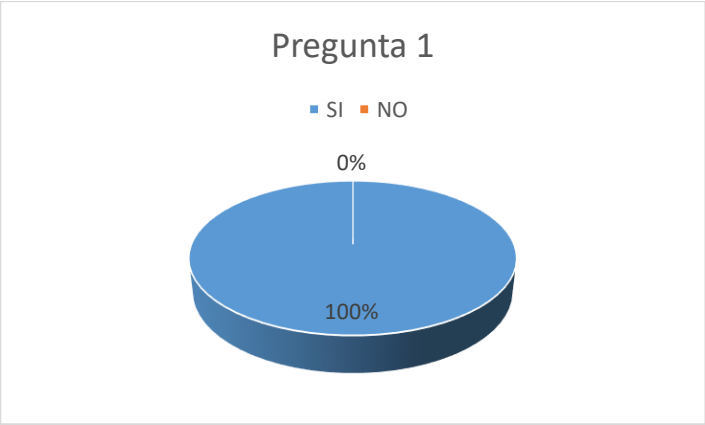
Tabla Nro. 1: Cuadro estadístico pregunta 1

Respuesta	Frecuencia	Porcentaje
SI	30	100%
NO	0	0%
TOTAL	30	100%

Fuente: Profesionales del Derecho en libre ejercicio de la Profesión

Autor: Juan Efrén Jumbo Condolo

Ilustración Nro. 1: Representación gráfica pregunta 1



Interpretación:

En base a los resultados arrojados por la primera pregunta se puede evidenciar que treinta (30) profesionales del derecho, lo cual representa el 100% de la población encuestada, señalaron que tienen conocimiento sobre las normativas jurídicas que regulan todo el tema de los ciberdelitos, así como también que regulan la información de los usuarios dentro del sector financiero del país.

Análisis:

Tomando en consideración los resultados arrojados por la primera pregunta debo indicar que me encuentro de acuerdo con la mayoría de los encuestados los cuales corresponden al 100% de la muestra seleccionada; pues es de pleno conocimiento para las personas que nos dedicamos tanto al estudio del derecho como a su ejercicio el que todo el tema de delitos informáticos se regulan por medio del Código Orgánico Integral Penal y que la información de los usuarios se ampara en la Ley de Protección de Datos Personales, teniendo así que la muestra es la apropiada para desarrollar la presente investigación.

Segunda pregunta:

¿Considera necesario establecer, procesos que contengan normas y políticas en las entidades financieras, con la finalidad que se mantenga segura la información de los usuarios de la entidad?

Tabla Nro. 2: Cuadro estadístico pregunta 2

Respuesta	Frecuencia	Porcentaje
SI	30	100%
NO	0	0%
TOTAL	30	100%

Fuente: Profesionales del Derecho en libre ejercicio de la Profesión

Autor: Juan Efrén Jumbo Condolo

Ilustración Nro. 2: Representación gráfica pregunta 2

Interpretación:

En base a los resultados arrojados por la segunda pregunta y por unanimidad se puede evidenciar que treinta (30) profesionales del derecho, lo cual representa el 100% de la población encuestada, señalaron que necesario establecer, procesos que contengan normas y políticas en las entidades financieras, con la finalidad de que toda la información que se guarda y respalda en las diferentes instituciones del sector financiero se mantenga segura no se vulnere la información personal de los clientes o usuarios de la entidad.

Análisis:

Sin lugar a dudas dentro de este criterio me sumo a lo manifestado por la mayoría que representa el 100% de la población encuestada pues como un usuario de las diferentes instituciones bancarias que existen en el país, los datos personales de los usuarios es algo que debe ser plenamente protegido, en tal sentido que no cualquier persona debe poder acceder a dicha información, por ello es importante que se comiencen a utilizar procesos adecuados en el tratamiento de la información digital en relación a las diferentes normativas ISO que se encuentran establecidas para el correcto tratamiento de esta información.

Tercera pregunta:

¿Conoce usted si en las entidades financieras de la Economía Popular y Solidaria, mantienen reglas centradas en la ciberseguridad en cuanto a la información de sus usuarios para que ésta no sea vulnerada a través de un ciberataque?

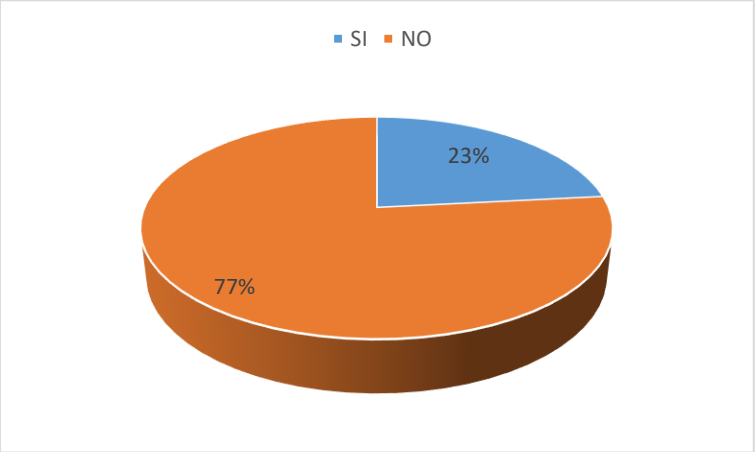
Tabla Nro. 3: Cuadro estadístico pregunta 3

Respuesta	Frecuencia	Porcentaje
SI	7	23%
NO	23	77%
TOTAL	30	100%

Fuente: Profesionales del Derecho en libre ejercicio de la Profesión

Autor: Juan Efrén Jumbo Condolo

Ilustración Nro. 3: Representación gráfica pregunta 3



Interpretación:

De la población encuestada en la tercera pregunta podemos obtener que una minoría, es decir siete (7) profesionales del derecho que representan el 23% de la muestra afirman que está protegida la información de los clientes en las entidades financieras, mientras que veintitrés (23) de los abogados en libre ejercicio de la profesión, que representan el 77% mencionaron que no se está protegiendo de manera adecuada la información de los usuarios

de las diferentes instituciones financieras, tomando en consideración sus diferentes experiencias personales.

Análisis:

Dentro de la presente pregunto tengo a bien manifestar que me encuentro en total desacuerdo con la minoría de las personas encuestadas que representan el 23% de la muestra; la razón principal de mi discrepancia se origina por cuanto si bien las instituciones financieras pueden llegar a tener buenas barreras de seguridad para la protección de los datos personales de las personas; estas no son del todo efectivas; provocando así que se vulneren las diferentes seguridades del sistema y por ende la información de los clientes cae a manos del ciberdelincuente para poder ejecutar las acciones que desea.

Por ello; me encuentro de acuerdo con lo que menciona la mayoría de la muestra encuestada; siendo esta el 77% de la muestra; pues es evidente la falencia de la protección de la información en las instituciones financieras debido principalmente a sus plataformas virtuales las cuales si bien están protegidas directamente por la institución; estas muy pocas veces están desarrolladas por ellas; lo que conlleva la participación de un tercero permitiendo de ese modo que se pueda dar el desvió de la información y posible interceptación para proceder a darles el uso que el ciberdelincuente desee conferirle.

Cuarta pregunta

¿Conoce usted si se ha efectuado algún ataque a los sistemas informáticos de cualquiera de las Instituciones Financieras?

Tabla Nro. 4: Cuadro estadístico pregunta 4

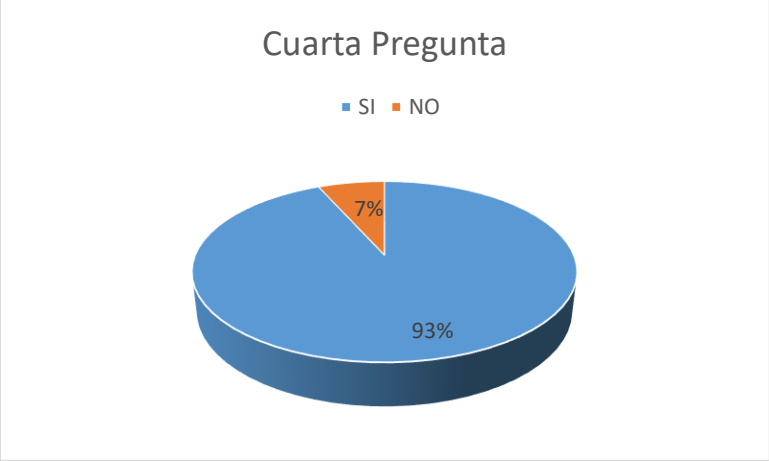
Respuesta	Frecuencia	Porcentaje
SI	28	93%

NO	2	7%
TOTAL	30	100%

Fuente: Profesionales del Derecho en libre ejercicio de la Profesión

Autor: Juan Efrén Jumbo Condolo

Ilustración Nro. 4: Representación gráfica pregunta



Interpretación:

Para la cuarta pregunta realizada a la muestra obtenemos que veintiocho (28) abogados en libre ejercicio de la profesión; mismos que representan el 93% de la muestra afirman que conocen de casos en los cuales se han podido evidenciar ciberataques los cuales han generado graves afectaciones e inconformidades con los diversos sistemas y la decepción llevada por cuanto las autoridades no actúan al respecto, mientras que como una minoría correspondiente a dos (2) abogados en libre ejercicio de la profesión que representan el 7% de la muestra nos dicen que no, pues no han revisado noticias tecnológicas en los últimos años por lo que se encuentran desinformados si ha existido o no alguno de estos ataques.

Análisis:

Tras el desarrollo de la presente presunta se denota una clara mayoría correspondiente al 93% en la cual me sumo a lo expuesto de las encuestas, dentro de lo concerniente a los ciberataques estos han ido en aumento dentro del país, provocando que ellos agarren más

fuerza conforme van pasando los años, es de considerar que no es un tema arraigado ni mucho menos que se encuentre oculto para la población, por lo que se puede denotar que dicho problema existe y lastimosamente va en crecida, también es de considerar que la mayoría de ciberataques que se ha escuchado son a empresas internacionales de gran renombre, aun con ello es de recordar que las Instituciones Financieras también han sufrido ataques internos.

Por otro lado, me encuentro en total desacuerdo con lo manifestado por la minoría que representa un 7% de la muestra encuestada, pues es claro que, si una persona o un ciudadano constantemente no revisare sus leyes o las noticias de su Estado, la posibilidad de caer en cualquier estafa compromete de manera seria su propia seguridad y con ello compromete su patrimonio.

Quinta pregunta:

¿Está de acuerdo con que se establezcan Lineamientos Propositivos centrados en la prevención, erradicación y control de los ciberataques contra los sistemas informáticos?

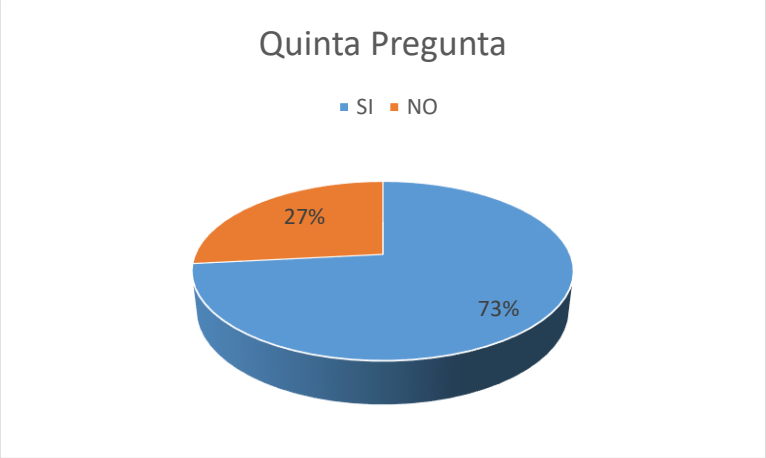
Tabla Nro. 5: Cuadro estadístico pregunta 5

Respuesta	Frecuencia	Porcentaje
SI	22	73%
NO	8	27%
TOTAL	30	100%

Fuente: Profesionales del Derecho en libre ejercicio de la Profesión

Autor: Juan Efrén Jumbo Condolo

Ilustración Nro. 5: Representación gráfica pregunta 5



Interpretación:

De la quinta pregunta realizada se puede evidenciar que veintidós (22) profesionales del derecho, lo cual representa el 73% de la población encuestada, señalaron que se encuentran de acuerdo con que se establezca de manera clara y precisa lineamientos propositivos a fin de regular los ataques a los sistemas, perseguir sus actuaciones y controlar las formas de prevención que mantiene el estado hacia los mismos; mientras que ocho (8) de los profesionales del derecho, que representan el 27% de la población encuestada indicaron que no se encontraban de acuerdo, pues si bien estos mecanismos podrían ayudar a reducir el índice de ataque por año, no solamente se requiere la propuesta sino que además se debe controlar la ejecución.

Análisis:

Para el presente caso en cuanto a lo relacionado a la mayoría en esta pregunta que corresponde al 73% de la población encuestada debo indicar que me encuentro de acuerdo con lo mencionado por parte de estos, ya que es evidente, pública y notoria la falta de control o regulación que existe por parte de las diversas instituciones miembros de la Economía Popular y Solidaria, sino que además estas no se encuentran trabajando en mejorar o reducir estos índices de peligro, por lo que claramente no existe la forma mediante la cual se pueda

proteger a estos sistemas y un lineamiento propositivo ayudaría a que estas instituciones mantengan una base firme para ejecutar sus actuaciones.

Por otro lado, me encuentro en total desacuerdo con la minoría dentro de la presente pregunta que representa el 27% de la muestra encuestada; principalmente porque los problemas que son generados por un ataque cibernético compromete la información de los ciudadanos y los bienes o patrimonio de estos, y las instituciones financieras sin una clara línea que perseguir no permite que estas instituciones se prevengan de los posibles ataques que se llegaren a suscitar en contra de sus sistemas.

6.2.Resultados de las entrevistas.

Para desarrollar una adecuada investigación dentro del presente Trabajo de Integración Curricular, se realizó dos entrevistas distintas; el público tomado en consideración para la primera entrevista fueron abogados que trabajan actualmente en entidades financieras conocedores del tema; una segunda muestra con otro formato de entrevista se lo desarrollo para un Agente Fiscal y para un Juzgador de la ciudad de Loja, mismos los cuales mantienen preguntas relacionadas en la tramitación de las causas.

6.2.1. Entrevistas a abogados de instituciones financieras.

Primera Pregunta:

Usted como funcionario de una entidad financiera y encargada de la defensa de los derechos de los funcionarios y clientes de esta entidad ¿Tiene conocimiento sobre vulnerabilidades de la información a los usuarios por medio de delitos informáticos en el ámbito financiero?

Primer entrevistado:

Efectivamente si tengo conocimiento, pues mi trabajo es velar por los derechos de los clientes y funcionarios de la entidad financiera, toda la información de los clientes es sumamente privada, algunas veces hemos tenido casos de intento de vulnerar la información privada es por eso que se mantiene un monitoreo constante a través de los compañeros de infraestructura tecnológica en la red y en caso que se intente vulnerar se envían alertas, así controlamos un poco estos ataques que se presentan.

Segundo entrevistado:

Muchos casos se han dado acerca de violar la información de los usuarios de las entidades financieras es por ello que hay un departamento de gestión de riesgos en calidad de seguridad de la información que detectan estas vulnerabilidades en ahí se registran muchos casos los cuales se evidencia los riesgos que corren los usuarios de la información que ellos proporcionan a la entidad.

Tercer entrevistado:

Los casos se presentan a diario en diferentes instituciones financieras la información no es segura en las entidades puesto que los hackers buscan minuciosamente métodos de como violentarla, estos casos se dan mediante medios electrónicos computadores, teléfonos etc., esta información puede ser proporcionada por los mismos usuarios ya que son estafados y engañados por tipos que empiezan a seguir a los mismos por redes sociales.

Comentario del autor:

En el presente caso nos encontramos con que los tres profesionales del derecho coinciden en que es un problema real existente y latente en el diario de los usuarios del sistema financiero, por lo que estos, gracias a su amplio conocimiento no solo en el área de las leyes sino que también en el ámbito de la informática han podido establecer un

mecanismo de protección, detección y prevención de los diferentes problemas de vulneración de la seguridad y posibles riesgos en los datos de los usuarios.

Segunda Pregunta:

En caso de que se presente en la entidad financiera casos de vulnerabilidad de la información ¿Estaría de acuerdo que se sancione con una pena privativa de libertad de 5 a 7 años según el Código Orgánico Integral Penal (COIP) Art. 233 a las personas que destruya o inutilice información clasificada de conformidad con la ley?

Primer entrevistado:

Estaría de acuerdo ya que toda información es privada y más aún si es de una entidad financiera, los clientes deben estar confiados y seguros que su información está segura, es por ello por lo que debe aplicarse el Art. 233 en el cual hace mención que sede sancionar con una pena de libertad de 5 a 7 años con esto se evitará que los clientes sean engañados violentando su información así mismo existen más artículos los cuales se deberían aplicar en los diferentes casos que se muestra vulnerable.

Segundo entrevistado:

La información clasificada está reservada por ley y es de carácter de confidencial para las personas particulares, estoy de acuerdo con la pena establecida en nuestro Código Orgánico Integral Penal, tenemos que considerar la participación en este delito.

Tercer entrevistado:

Parto de la idea, de que la norma sancionadora, no regula conductas humanas, ni protege bienes jurídicos, lo primero porque existe nuevos estudios basados en la neurociencia, que vislumbran la irracionalidad de establecer penas o sanciones a una persona, con el fin de rehabilitarlas y que puedan reinsertarse en sociedad. Segundo, no

protege bienes jurídicos porque la norma actúa tras una acción u omisión delictiva, es decir la norma nos recuerda que está vigente y nos indica de qué somos responsables. Pero un delincuente no revisa la norma para delinquir, lo hace con o sin ella, en vigencia o derogada, con pena capital como sanción o con la mínima sanción.

Comentario del autor:

Para la segunda pregunta encontramos que dos de los profesionales entrevistados mencionan estar de acuerdo con la pena establecida dentro del art. 233 del Código Orgánico Integral Penal; pues con ella se puede llegar a buscar una adecuada protección de los derechos de las personas que son víctimas de este tipo de delitos al igual que garantizan la protección de la Institución financiera como tal; mientras que uno de los entrevistados nos da a entender una idea totalmente distinta en cuanto a la aplicación no solo de la pena sino que también cuestiona la necesidad de la misma, apegándose a que no se requiere necesariamente a la aplicación de una pena más grave; pues el infractor no revisara la normativa previo a delinquir lo que provoca que de manera directa no tenga relación la pena con la conducta; en el presente caso discrepo de lo mencionado por los entrevistados; pues a mí criterio la proporcionalidad en cuanto a los daños efectuados no solo a la institución sino que también a los usuarios de esta institución no llega a compensar en múltiples ocasiones por cuanto al eliminar información el recuperarla es prácticamente imposible; por lo que devenga gastos millonarios para la institución financiera que no serán respondidos por el presunto infractor.

Tercera Pregunta:

¿Considera necesario establecer, procesos que contengan normas y políticas en las entidades financieras, con la finalidad que se mantenga segura no se vulnere la información de los clientes o usuarios de la entidad?

Primer entrevistado:

Definitivamente, se debe invertir en seguridad informática, para prevenir su mal o indebido uso, pues como usuarios pertenecemos al grupo de atención prioritaria y el Estado tiene la obligación de reforzar nuestra seguridad en sentido amplio, no se diga nuestra información que reposa en bases de datos a las que confiamos su reserva.

Segundo entrevistado:

Estoy de acuerdo ya que en las entidades financieras deberían tener procesos de calidad los mismos que contengan normas y políticas muy reforzadas y orientadas a la seguridad de la información esto evitara que se vulnere la misma, tanto para los clientes como para la entidad, estos procesos deben cumplirse de manera correcta para que tengan buenos resultados y a si los clientes confíen en la entidad y en sus ahorros están bien protegidos.

Tercer entrevistado:

Si, toda entienda financiera debe contar con una rigurosidad sobre la seguridad de la información de los usuarios, es por ello que se debe hacer cumplir estas leyes, se debería elaborar procesos que los lleven a tener una calidad en la entidad financiera y así robustecer la seguridad de la misma, y que los clientes estén conformes y tranquilos.

Comentario del autor:

Una vez más se cuenta con unanimidad, pues los tres profesionales del derecho han llegado a la conclusión de que no solo se debe proceder con programas necesarios para evitar la vulneración de la información de los clientes, debiendo de esta manera reforzar la seguridad de los mismos, sino que además es necesario que se potencie y se busque un mayor control al momento de ejecutar estos programas; por eso no solo instan a reforzar los procedimientos que mantienen a la hora de conferir información a terceros; sino que

además se debe buscar elevar la calidad de la institución financiera por respetar un debido proceso y así mantener de mejor manera los distintos servidores mediante los cuales se protege la información digital de los usuarios; con ello se ha logrado demostrar que existe una falencia a la hora de buscar y trabajar con los datos de los usuarios, debiendo reforzar la seguridad de esta información.

Cuarta Pregunta:

¿Conoce usted si en las entidades financieras, está suficientemente protegida la información de sus clientes o usuarios para que ésta no sea vulnerada?

Primer Entrevistado:

Hay entidades financieras que tienen cierto grado de seguridad, o al menos al usuario lo hacen sentirse seguro, sin embargo, para establecer tal grado de seguridad se necesita un profesional experto que pueda brindar información al usuario respecto a sus datos, los que deben ser y estar vigilados y controlados únicamente por la entidad financiera a quién los préstamos y autorizamos.

Segundo Entrevistado:

La información de los usuarios y clientes de entidades financieras aún se encuentran desprotegidas y en estos últimos años han aumentado los ataques informáticos dentro del ámbito financiero, prueba de ello podemos deducir claramente que aún existe deficiencias en el manejo de la información.

Tercer Entrevistado.

Existen entidades financieras que ofrecen un nivel de seguridad considerable, proporcionando a los usuarios una sensación de confianza. Sin embargo, para garantizar este nivel de seguridad, se requiere la intervención de profesionales expertos que puedan informar

a los usuarios sobre la protección de sus datos. Estos datos deben ser gestionados y controlados exclusivamente por la entidad financiera a la que autorizamos el acceso y los préstamos.

Comentario del autor:

Pese a considerar los tres entrevistados que si existen un cierto grado de confianza por parte de la institución hacia sus clientes se puede notar que estos aun aseveran que no es suficiente esta protección conferida; si no que por el contrario, esta protección no llega a ser suficiente lo que ha conllevado que muchos usuarios sufran perdida de su información debido al claro incremento en el cometimiento de estos delitos; llevando así una situación en la cual por desconocimiento no se puede ejecutar ninguna acción tendiente a proteger su patrimonio o su información; por lo que es necesario reforzar esta seguridad.

Quinta Pregunta:

¿Está usted de acuerdo que se debería mejorar la seguridad del sistema penal ecuatoriano referente a la violación de la información de los usuarios dentro de las entidades financieras?

Primer Entrevistado:

Como lo referí anteriormente, la norma penal, no previene las conductas humanas, toda vez que cada persona procede sin revisar la pena privativa de libertad establecida para determinado delito, por ello es infructuoso pensar que, si agravamos penas, tendríamos una mejor seguridad. Por ello, sostengo que dé debe trabajar desde otra perspectiva, como medidas preventivas eficientes y, de hecho, para prevenir este tipo de delitos informáticos.

Segundo Entrevistado:

Las leyes que rigen a nuestro país deben mejorar constantemente en beneficio de las personas, por lo que necesitamos un cambio que garantice a los usuarios y clientes que la información que es la confianza de las personas con las diferentes entidades bancarias está segura y no sea vulnerada.

Tercer Entrevistado.

Si, el derecho informático es una rama hoy en día se la debe tomar en cuenta, ya que a medida que avanza la tecnología también avanzan los delitos que comenten las personas que utilizan estos medios informáticos, es por ello que la normativa penal debe amparar a los usuarios.

Comentario del autor.

Se puede evidenciar que la mayoría de los entrevistados, sus respuestas tienen bastante relación en cuanto a la seguridad de la información para que esta no sea vulnerada, así como también que se busque procesos de calidad que contengan normas y políticas en las entidades financieras las cuales permitirán robustecer la seguridad de la información de los clientes.

6.2.2. Entrevistas a jueces y fiscales de la ciudad de Loja.

Primera Pregunta:

¿Qué tan común es que avoque conocimiento por un delito informático?

Primer entrevistado:

Los delitos informáticos dentro de la tramitación de las causas no son tan comunes de investigar y por lo tanto el procedimiento que se llega a seguir muchas de las veces presentan complicaciones a la hora de poder llevar una correcta investigación, los ciberdelitos como tal contenidos en el COIP no son tan comunes, aun con ello el hecho que no sean comunes no

quiere decir que no se tramiten, en mi campo de acción investigue alrededor de unos 3 o 4 noticias del delito por ataque a la integridad de los sistemas informáticos, principalmente al sistema de la Agencia Nacional de Transito mediante la cual procedieron a realizar traspasos de dominio de vehículos desde un usuario hackeado

Segundo entrevistado:

En realidad, el conocimiento de un ciberdelito pocas veces llega a conocimiento el Órgano Jurisdiccional, por cuanto pocos agentes fiscales conocen la manera en la cual se debe ejecutar estas investigaciones, es importante tomar en consideración que existen formas para poder investigar estos delitos y que estos deben ser lo menos intrusivos y restrictivos de derechos posible.

Comentario del autor:

Ambos entrevistados destacan que el avocar conocimiento por este tipo de delitos es muy poco común, uno de ellos principalmente ha señalado por cuanto tienen una múltiple cantidad de complicaciones a la hora de poder investigar estos delitos, con ello al limitarse su accionar es normal que las causas no sean investigadas de correcta manera, el segundo de los entrevistados ha indicado que estos delitos no suelen llegar a conocimiento de la autoridad jurisdiccional, principalmente por cuanto no se logra recopilar los medios probatorios necesarios para poder ejecutar o imputar una acción penal. Con ello podemos evidenciar que existe una clara falencia en el momento de investigar estos delitos.

Segunda pregunta:

Para la recopilación de la evidencia ¿Qué lineamientos siguen?

Primer entrevistado:

Como primer alcance de la persona que interpone la denuncia se le solicita que estos datos en caso de ser a través de mensajes de texto o de tratarse de un acceso no permitido se requiere que se realice una captura de pantalla de lo que le arroje su dispositivo, lo cual es añadido al expediente fiscal y con ello se investiga, ahora bien, esto no garantiza la integridad de la información ni mucho menos que esta sea veraz, por lo que en el transcurso de la investigación se solicita el dispositivo mediante el cual se elaboró o se obtuvo la información, el cual es ingresado a cadena de custodia para proceder a la extracción integra del contenido de los datos necesarios.

Segundo entrevistado:

El procedimiento adecuado es desde el primer momento en el que Fiscalía toma conocimiento del cometimiento de un presunto delito cibernético proceda al secuestro del medio en el cual se presume se haya cometido la infracción para iniciar la respectiva cadena de custodia y evitar que la información pueda perderse, lastimosamente esto no se elabora de esa manera ya sea por la falta de colaboración de la víctima, policía judicial o incluso por la misma negligencia de los agentes fiscales, por lo que esa evidencia ya puede sufrir alteraciones y en un caso como lo es los ciberdelitos se puede eliminar la información desde otro dispositivo, provocando asi que fiscalía no pueda recopilar los elementos de convicción necesarios y dejando en la impunidad a los presuntos infractores.

Comentario del autor:

De ello podemos destacar que nos encontramos con dos opiniones bastante concretas a la hora de determinar el actuar de cada una de los órganos de la función jurisdiccional, principalmente encontramos con una situación en la cual se trata de reducir a escrito lo dispuesto por parte del agente fiscal en su afán de investigar de la mejor manera posible, mientras que por otro lado por parte del juzgador alega que esta situación conlleva a que la

administración de justicia sea ineficiente a la hora de aplicar la norma, está más que claro que el accionar de uno de los órganos jurisdiccionales no permite que se continúe con el proceso adecuado, principalmente es de entender que siempre va a existir cierto tipo de diferencias entre el accionar del agente fiscal con el accionar del juzgador, la preservación de las evidencias es sin lugar a dudas uno de los pilares fundamentales a la hora de que una evidencia o prueba pueda ser considerada como válida por lo que su proceder debe siempre aferrarse a lo que mejor favorezca a la investigación penal.

Tercera pregunta:

¿Considera usted que las sanciones estipuladas para los ciber-delitos son proporcionales a la conducta generada?

Primer entrevistado

La complejidad de la investigación a en los ciberdelitos es muy alta, las sanciones las cuales se encuentran estipuladas por parte del Código Organico Integral Penal en base a la complejidad del caso y el bien jurídico afectado no llegan a ser proporcionales, supongamos el caso que se elimine por completo un sistema informático, en esa situación los ingenieros y todo el personal que trabajo en su desarrollo queda totalmente afectado y no solo eso sino que el tiempo invertido y los recursos demandados por parte de la empresa no llegan a ser reparados en su totalidad

Segundo entrevistado

Hay que tener en cuenta una situación, la proporcionalidad se devenga en cuanto a que la conducta cometida y la pena impuesta sean proporcionales, pero esta proporcionalidad se encuentra limitada en el aspecto del tipo penal y la conducta que de este demande, como juzgador no se podrá bajo ninguna circunstancia presentar una pena privativa o una sanción que no se encuentre tipificada, es muy importante que la proporcionalidad sea analizada por

los legisladores, pues las sanciones impuestas y las afectaciones que provocan por los bienes jurídicos afectados lastimosamente no son acordes

Comentarios del autor.

Nos encontramos claramente con una posición de inconformidad por parte tanto del juzgador como del agente fiscal entrevistado, el primero de ellos al determinar que la investigación y todas las gestiones que demandan este tipo de delitos no llega a ser proporcional a la pena que se impone por lo que se debería reforzar las sanciones que se aplican, el segundo de ellos nos da un panorama más apegado en cuanto a derecho corresponde manifestando que aunque se desee imponer una sanción más grave, esta no sería aceptada principalmente por la tipificación de la norma, es importante analizar estas posiciones jurídicas y en base a ello lograr afianzar la legislación ecuatoriana para poder tomar medidas necesarias en la tramitación de las causas penales

Cuarta pregunta:

¿Cuál considera usted que sería un buen procedimiento para la investigación de los ciberdelitos?

Primer entrevistado

El procedimiento se tramita de la manera correcta y depende mucho del criterio de cada agente fiscal, mientras se respeten las garantías básicas del debido proceso el agente fiscal puede proceder conforme mejor lo creyere conveniente.

Segundo entrevistado

Existen garantías básicas en el procedimiento que deben ser respetadas a cabalidad, ya sea como por ejemplo las cadenas de custodia, la autorización judicial para extracción de información, todos estos procedimientos deben ser debidamente respetados y bajo ninguna

circunstancia se puede vulnerar a los mismos, por ende, si no se respeta estas formalidades sustanciales no se podrá continuar con el transcurso óptimo de la investigación y por consiguiente estos no se podrán sancionar

Comentarios del autor.

De esta pregunta destacamos la importancia que tiene el criterio de los agentes fiscales a la hora de disponer cual es el procedimiento adecuado a la hora de poder investigar un delito de esta magnitud, es más que claro que existen formalidades o procedimientos propios de cada uno de los procedimientos y existen formalidades que ser cumplidas, como por ejemplo el hecho de requerir que los documentos o dispositivos electrónicos ingresen bajo una cadena de custodia, es más que claro que estos procedimientos deben respetarse y siempre y cuando se respeten las garantías del proceso que ampara la tramitación de las causas estas investigaciones no tienen por qué mantenerse en proceso de espera.

Quinta pregunta:

¿Qué solución usted le daría al problema planteado?

Primer entrevistado

En cuanto a su problema de investigación es muy importante que se busque la forma en la cual no solo se sancione a la persona investigada sino que tambien se cree una Unidad Especializada para esta investigación por parte de los agentes de la Policía Nacional, porque la misma Policía Judicial o la misma Unidad de Criminalística no puede ejecutar todas las acciones de lo que conlleva un delito informático, con una unidad especializada como lo hay en República Dominicana, la acción e investigación de estos delitos será más ágil y por la tanto la forma en la cual se detiene el accionar de estos individuos es mucho más efectiva

Segundo entrevistado

Es un tema de investigación bastante bueno y considero que las acciones no deben ser tomadas solo en cuanto el endurecimiento de las penas sino que se debe reforzar la etapa de prevención del delito, cabe destacar las acciones que han ido tomando las instituciones financieras enviando los correos electrónicos de aviso a sus usuarios, es de vital importancia que se trabaje en ese sector, alertar a la ciudadanía a través de los medios digitales y las redes sociales para asi evitar que las personas que pretenden vulnerar la normativa se aproveche de la ciudadanía que no conoce sobre los medios digitales

Comentarios del autor.

De los entrevistados destacamos que se realizan varios requerimientos muy puntuales, principalmente destacamos la necesidad de que se establezca una Unidad Especializada para la investigación de ciberdelitos y que su importancia sea a nivel de todas las ciudades y provincias del pais para de esa manera garantizar el correcto trato de la evidencia digital, además de ello por parte de las instituciones financieras se debe reforzar la educación digital en cuanto a la prevención de que sus usuarios sean víctimas de alguno de estos delitos, finalmente es de tomar en consideración que de igual manera un endurecimiento en la normativa puede ser aplicado por cuanto la proporcionalidad en cuanto al delito cometido y el daño generado no es de acorde a los bienes jurídicos protegidos, siempre y cuando esta vulneración sea demostrada en el momento procesal oportuno.

6.3. Estudio de casos

6.3.1 Caso número uno Noticia

1. Datos referenciales.

Título: EL COMERCIO

Autor: Anónimo. Diario El Comercio

Tema: Política

Título: Mintel pidió a Banco Pichincha informar sobre el grado de vulnerabilidad por ataque cibernético

Fecha: 13 de octubre de 2021; 19:00

2) Contenido

La ministra de Telecomunicaciones y de la Sociedad de la Información (Mintel), Vianna Maino, acudió este 13 de octubre del 2021 al llamado de la Comisión de Desarrollo Económico de la Asamblea Nacional, que busca conocer las causas y consecuencias de la inhabilitación de los servicios bancarios del Banco Pichincha.

La funcionaria señaló que, el pasado 11 de octubre, después de que el Banco Pichincha informó que la falla en el acceso y prestación de los servicios se debió a un "incidente de ciberseguridad" detectado en sus sistemas informáticos, el Mintel le solicitó a la Superintendencia de Bancos y al gerente de la entidad bancaria se den a conocer el estado real del ataque cibernético y el grado de cumplimiento de las medidas de respuesta a dicho incidente.

Específicamente, le solicitó al gerente del Banco Pichincha que informe a la Dirección Nacional de Registro de Datos Públicos (Dinardap), que, si por el incidente registrado se ha vulnerado el derecho de protección de datos personales, pero aún no han sido respondida la solicitud, dijo Maino.

Además, se le ofreció la colaboración e intervención para verificar el cumplimiento de lo que manda la Ley Orgánica de Protección de Datos Personales, vigente desde mayo de este 2021, agregó.

Además, la funcionaria señaló que esta Cartera de Estado se dedica a la prevención de los delitos de ciberseguridad y establece las directrices que buscan afianzar un ciberespacio seguro. Pero, que el control sobre entidades del sector financiero no le corresponde al Mintel.

Sin embargo, señaló que el pasado 5 de agosto ya remitió a la Superintendencia de Bancos y a todas las instituciones del sector público, "recomendaciones selectivas y correctivas de ciberseguridad para evitar eventuales afectaciones o posibles ataques cibernéticos a las entidades del Estado".

La funcionaria señaló que, se le remitió a la Superintendencia de Bancos la solicitud de que eleven sus medias de seguridad al más alto nivel posible y además se le recomendó cómo hacerlo, dijo.

La Comisión Legislativa, presidida por el asambleísta Daniel Noboa Azin, convocó el 12 de octubre a 14 personas, entre las que constaban autoridades, el representante del Banco Pichincha y de otras empresas privadas para que comparezcan esta tarde en la Asamblea Nacional, la mayoría se excusó de participar.

Noboa señaló "que es de suma importancia conocer qué sucedió con el sistema financiero del Banco Pichincha y conocer el grado de vulnerabilidad que tienen los datos personales, para tomar medidas pertinentes de manera oportuna".

Antonio Acosta, presidente Directorio del Banco Pichincha, también estaba convocado la tarde de este 13 de octubre, pero no compareció.

Igualmente, la Superintendencia de Bancos no llegó a la Asamblea. El organismo de control señaló que se encuentra en pleno proceso de supervisión y que no cuenta con las debidas conclusiones de los procedimientos de control en curso, por lo tanto, "no se pueden adelantar criterios".

Marco Rodríguez, vicepresidente de la Asociación de Bancos Privados (Asobanca), tampoco acudió a la invitación de la Comisión. Señaló que el corto tiempo con el que se hizo la convocatoria le impidió comparecer.

3) Comentarios del autor

Para prevenir y mitigar estas vulnerabilidades, las entidades financieras suelen implementar medidas de seguridad como el cifrado de datos, autenticación de dos factores, sistemas de detección de intrusiones, actualizaciones de software regulares, capacitación en seguridad para empleados y monitoreo constante de la actividad sospechosa en los sistemas.

Es importante destacar que la seguridad de la información es un desafío constante y que las entidades financieras deben estar al tanto de las últimas amenazas y seguir mejores prácticas en seguridad cibernética para proteger los datos de sus clientes.

6.3.2. Caso número dos, Noticia

1) Datos referenciales

Título: EL COMERCIO

Autor: Anónimo. Diario El Comercio

Tema: Informática

Título: 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020

Fecha: 25 de julio de 2022

2) Contenido

La investigación policial duró 11 meses. Luego de rastrear información por medios electrónicos y hacer un análisis de redes digitales, la Policía detuvo a tres presuntos ciberdelincuentes que se dedicaban a estafar en línea.

Durante un operativo, las tres personas fueron aprehendidas la madrugada del 2 de junio pasado. Según las pesquisas, ellos habrían creado una página web y una plataforma de comercio electrónico por redes sociales falsas. Operaban desde Pichincha y Manabí.

Agentes a cargo de este caso detallaron que los sospechosos usaban esos medios digitales para promocionar y vender artículos electrónicos a bajos precios.

Las víctimas se contactaban con ellos para adquirir esos artefactos y les depositaban el dinero en cuentas bancarias. Tras recibir el dinero, los presuntos ciberdelincuentes bloqueaban el contacto con los afectados y jamás enviaban el artículo solicitado.

Los ataques de las cibermafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3 183 delitos informáticos. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1 851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650 investigaciones a escala nacional.

Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias con más casos.

Gonzalo García, jefe de la Unidad de Ciberdelitos, dice que este tipo de hechos delictivos ocurren porque las personas tienen más acceso a Internet y redes sociales. Cifras oficiales muestran que el 79,21% de la población ecuatoriana tiene acceso a la web y alrededor de 15,8 millones de personas en el país tienen cuentas en las diferentes redes sociales.

Un informe de la Interpol (Policía Internacional) también menciona que “el mundo está más conectado digitalmente que nunca. Los delincuentes están aprovechando esa transformación en línea para atacar, a través de las redes y sistemas informáticos”.

3) Comentario del autor:

Los ciberdelitos claramente se encuentran en subida, ello no quiere decir que estos no puedan llegar a ser controlados, es necesario para la ejecución de una adecuada protección de

los usuarios de las diferentes redes el poder protegerlos gracias a personal especializado en la investigación de este tipo de delitos, con la presente noticia podemos destacar que si es posible el darle persecución a los presuntos infractores, todo ello gracias a las herramientas de rastreo necesarias y con la suficiente capacidad es posible determinar e inclusive capturar in flagranti a las personas que cometen este tipo de acciones en contra de los ciudadanos.

6.3.3. Caso número tres, Noticia

1) Datos referenciales

Título: EL COMERCIO

Autor: Anónimo. Diario El Comercio

Tema: Negocios

Título: Banco Pichincha confirma 'incidente de ciberseguridad' en sus sistemas

Fecha: 11 de octubre de 2021

2) Contenido

Después de más de 72 horas sin servicio en sus canales electrónicos, el Banco Pichincha informó en un comunicado que la falla se debe a un "incidente de ciberseguridad" detectado en sus sistemas informáticos.

El comunicado lo publicó el banco a través de su cuenta de Twitter la tarde de este lunes 11 de octubre de 2021.

"Hemos tomado acciones inmediatas como aislar los sistemas potencialmente afectados del resto de nuestra red y contar con expertos de ciberseguridad para asistir en la investigación".

Hasta el momento, el banco no ha informado acerca del tipo de ciberataque al cual sus sistemas estuvieron expuestos ni ha especificado en qué sector de su infraestructura se registra la falla.

La red de cajeros continúa funcionando

El banco aseguró que de momento su red de cajeros automáticos para retiros y pagos con tarjeta se encuentra habilitada.

“Este incidente tecnológico no afecta el desempeño financiero del banco. Reiteramos nuestro compromiso en precautelar los intereses de nuestros clientes y restablecer la atención normal a través de nuestros canales digitales en el menor tiempo posible”, recalcó la institución en el comunicado.

Varias fallas de seguridad en 2021

En febrero de 2021, medios de comunicación informaron acerca de una filtración masiva de datos personales de sus clientes. Esto, después de que el banco asegurara que en redes sociales circulaba información falsa al respecto.

Después de estas publicaciones, el Banco Pichincha reconoció que hubo “un acceso no autorizado a los sistemas de un proveedor que presta servicios de mercadeo del programa pichincha Miles”.

En esa ocasión, la filtración llevada a cabo por el grupo de ciberdelicuentes Hotarus Corp comprometió los datos personales de miles de clientes del banco y de Grupo Diners.

En un inicio, el grupo exigió un pago millonario para el rescate de esos datos. El pago nunca se dio y meses después la base de datos circulaba en foros hackers.

En julio de este año, Hotarus Corp volvió a aparecer en foros de Internet. El grupo, esta vez, liberó de manera gratuita la base de datos completa.

La veracidad de esta fue dada a conocer en un informe de La Posta publicado en esos días. Hoy, esa información está disponible en varios sitios de la ‘deep web’ para descarga libre.

En esa ocasión, la entidad respondió que sus sistemas “no han sido vulnerados en ningún momento como se ha difundido en las últimas horas”.

Según la versión del banco, se trataba de la misma base de datos que había sido robada a un proveedor en febrero y por la cual existía una denuncia en Fiscalía.

El comunicado insistía en que no existió ningún tipo de acceso no consentido a los sistemas del banco, mientras que el grupo hacker afirmaba lo contrario.

3) Comentario del autor:

Dentro de la presente noticia nos encontramos principalmente con una circunstancia o situación en la cual el Banco Pichincha, una de las instituciones financieras más grandes del país se ve inmersa en un ciberataque lo que conlleva a que la seguridad de la información de los usuarios haya sido afectada y que además de ello los datos de ciertas personas hayan sido expuestos, con ello no solamente nos da a notar la falta de capacitación existente dentro de los sectores de la sociedad en cuanto a la prevención de un ataque cibernético, sino que además nos indica la falencia de las instituciones bancarias a la hora de hacer algo para prevenir las afectaciones a sus sistemas, sin lugar a dudas nos deja en clara que es necesario el trabajar en mejorar los sistemas de seguridad informática de los bancos e instituciones financieras así como también trabajar en fortalecer las debilidades de los mismos.

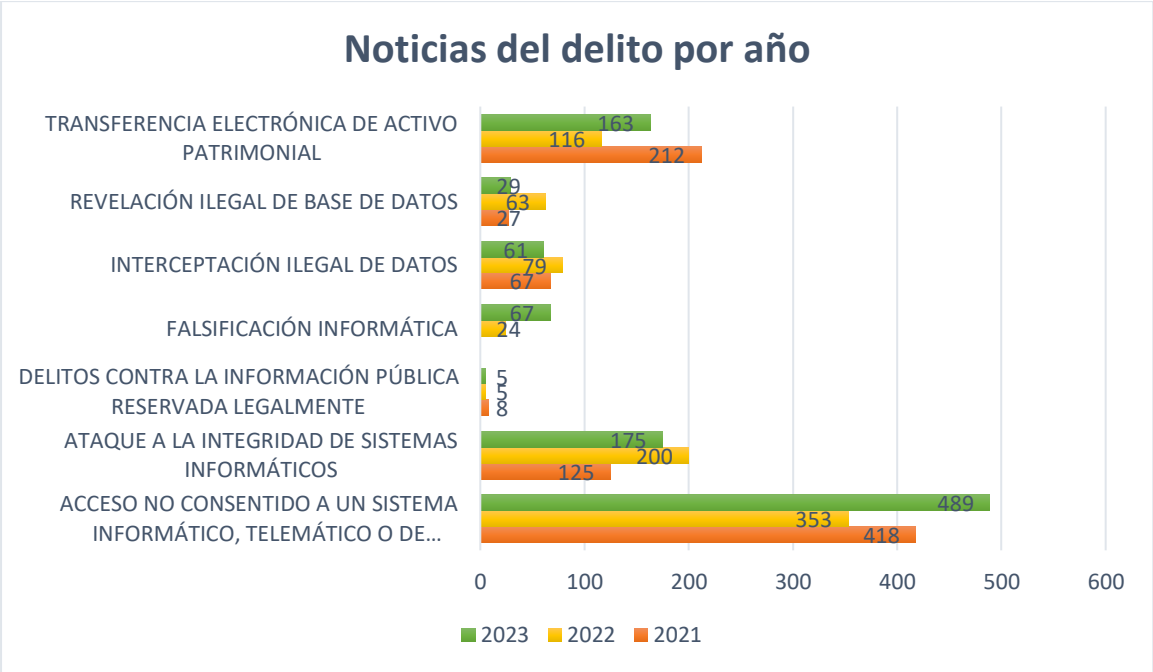
6.4. Datos estadísticos

Para el desarrollo del presente subtema se investigó y obtuvo información oportuna con datos estadísticos acerca de las Noticias del Delito puestas a conocimiento de la Fiscalía

por los tipos penales de revelación ilegal de base de datos; interceptación ilegal de datos; transferencia electrónica de activo patrimonial; ataque a la integridad de sistemas informáticos; delitos contra la información pública reservada legalmente; acceso no consentido a un sistema informático, telemático, o de telecomunicación; y, falsificación informática, con lo cual se analiza e interpreta la siguiente información:

6.4.1. Noticias del Delito puestas a conocimiento de la Fiscalía por delitos informáticos.

Ilustración Nro. 6



Fuente: Fiscalía General del Estado, Dirección de Estadística y Sistemas de Información.

Autor: Juan Efrén Jumbo Condolo

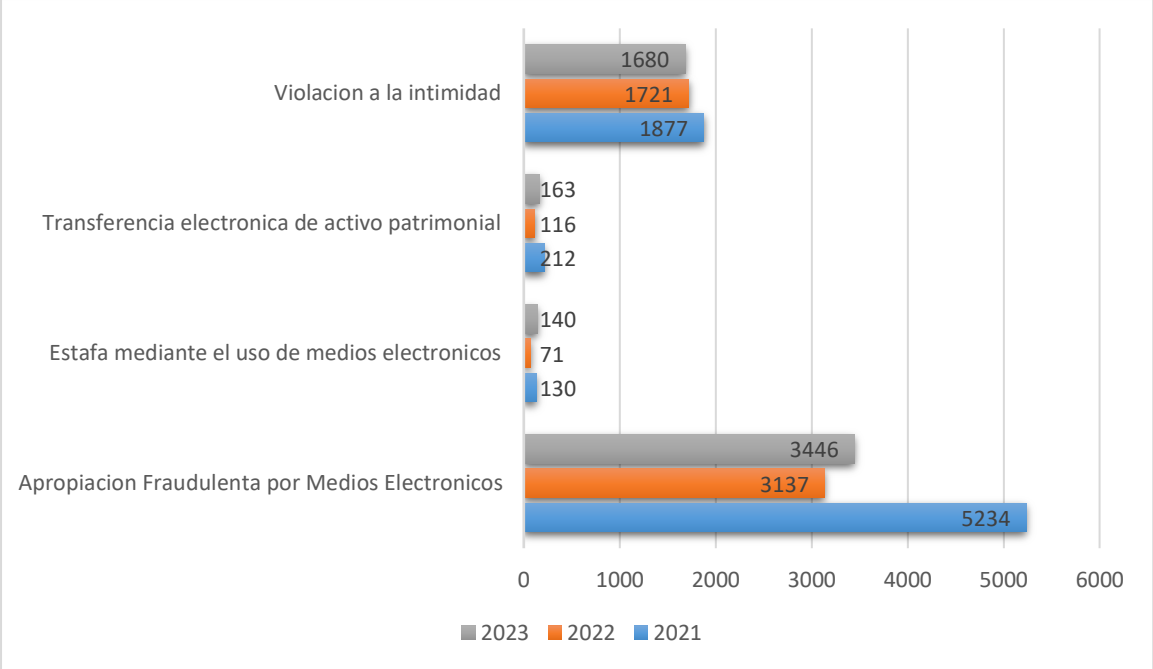
Interpretación y análisis del autor.

Con la información recopilada a través de la Dirección de Estadísticas y Sistema de Información de la Fiscalía General del Estado hemos podido llegar a identificar la cantidad de noticias del delito puestas a conocimiento por el cometimiento de los presuntos delitos de Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, Ataque

a la integridad de los sistemas informáticos, delitos contra la información pública reservada legalmente, falsificación informática, interceptación ilegal de datos, revelación ilegal de base de datos y transferencia electrónica de activo patrimonial durante los años 2021, 2022 y 2023 en el Ecuador, de esto podemos obtener varios datos importantes, principalmente destacamos que el ciberdelito que más se comete a nivel Nacional es de Acceso no Consentido a un Sistema Informático, Telemático o de Telecomunicaciones, llegando a ser estos para el año 2021 un total de cuatrocientos dieciocho noticias del delito (418); para el año 2022 reduciéndose a trescientos cincuenta y tres noticias del delito (353) e incrementando para el año 2023 a un total de cuatrocientos ochenta y nueve noticias del delito (489) siendo este uno de los delitos más cometidos en contra de los sistemas informáticos a nivel nacional. Destacamos así mismo que el Ataque a la Integridad de Sistemas Informáticos es de igual manera uno de los ciberdelitos que más se cometen, siendo el 2022 el año que más se ha denunciado este delito con una cantidad de 200 noticias del delito. Finalmente, es de tomar en cuenta que el delito de Transferencia Electrónica de Activo Patrimonial es otro de los delitos que más se han denunciado, siendo en este caso el año de 2021 el que más ha tramitado este tipo de causas llegando a un total de 212 noticias del delito, con ello se ha logrado determinar que este tipo de conductas pese a ser muy específicas en cuanto a los requisitos indispensables de tipicidad, antijuricidad y culpabilidad, no llegan a ser noticias ampliamente investigadas lo que deja en marco de duda si se está adecuando las conductas al tipo penal correcto o las noticias del delito que deberían ser tramitadas por estos tipo penales no se están desarrollando por cuanto no se las configura como tal.

6.4.2. Noticias del Delito puestas a conocimiento de la Fiscalía por delitos cometidos a través de medios telemáticos.

Ilustración Nro. 7



Fuente: Fiscalía General del Estado, Dirección de Estadística y Sistemas de Información.

Autor: Juan Efrén Jumbo Condolo

Interpretación y análisis del autor.

Si bien es cierto existen la categoría de los ciberdelitos en general, también existen delitos comunes los cuales pueden ser cometidos gracias al uso de los medios tecnológicos, tal es el caso de cuatro tipos penales como lo son la Apropiación fraudulenta por medios electrónicos, Estafa mediante medios electrónicos, transferencia electrónica de activo patrimonial y delito de violación a la intimidad, delitos los cuales juegan un papel muy importante en las causas presentadas ante la fiscalía, en cuanto al delito más común de estos es el de Apropiación Fraudulenta, mismo en el cual el presunto infractor mediante engaños logra apropiarse de un activo patrimonial de alguna persona, siendo un delito bastante tramitado, llegando a tramitarse dentro del año 2021 un total de 5234 noticias del delito siendo uno de los años más elevados en los últimos 3 periodos, esto se puede deber principalmente a que en dicha época se encontraba no solo el país sino que además el mundo entero atravesando la pandemia del Covid-19 una pandemia de carácter mundial la cual vendría a afectar a todos los sectores de la sociedad provocando que muchas empresas y

microempresarios se vean en la necesidad de reducir sus consumos o incluso en ciertos casos buscar la forma de invertir en nuevos sectores productivos dentro de su misma área; lo cual fue un foco de atención para los ciberdelincuentes y una zona en la cual podían explotar sus propuestas y sus finalidades. Otro de los delitos que más se ha denunciado e investigado es el delito de la Violación a la Intimidad, de igual manera en el año 2021 es el año con más investigaciones por este tipo penal, alcanzando la cifra de 1877 noticias del delito, por lo que nos da a notar la falta de conciencia de las personas a la hora de exponerse a través de los medios digitales y redes sociales, estos datos estadísticos nos dan a conocer cuál es la situación de los demás delitos que si bien no se encuentran tipificados como ciberdelitos pero su comisión es a través de los medios telemáticos lo que genera que sean analizados como una categoría independiente.

7. Discusión.

Luego de haber analizado y verificado la información obtenida durante la investigación mediante encuestas y entrevistas de acuerdo a la metodología planteada se abre paso a la discusión de la información recabada, donde se procederá a verificar cada uno de los objetivos planteados.

7.1. Verificación de los objetivos

7.1.1. Objetivo General

El objetivo general planteado es el siguiente:

Analizar un estudio jurídico y derecho comparado de las vulnerabilidades de la información a los usuarios basados delitos informáticos en el sistema financiero popular y solidario.

El objetivo general que se planteó para el trabajo de Integración Curricular, se puede destacar durante el desarrollo del marco teórico el cual se realizó con mucha minuciosidad, el estudio de la vulnerabilidad de la información en las entidades financieras en nuestro país desde una perspectiva de derecho comparado implica analizar cómo la legislación y las regulaciones en Ecuador abordan este tema en comparación con otros países. Esto es especialmente relevante dada la creciente importancia de la ciberseguridad en el ámbito financiero.

Tomando en consideración en un marco legal en nuestro país se basa en la descripción de las leyes y regulaciones relevantes en Ecuador que se ocupan de la ciberseguridad y la protección de datos en el sector bancario, así como también a identificación de leyes específicas relacionadas con la seguridad cibernética y la prevención de delitos informáticos en instituciones financieras, principalmente destacamos a la Constitución de la República del Ecuador como norma suprema de conformidad al Art. 424 y 425 ibídem, en la constatamos la

existencia de una garantía y derecho a los ciudadanos en cuanto a la protección de sus datos personales y como consumidores de un servicio el poder contar con situaciones y garantías de seguridad en base a la información que proporcionan, como normativas internacionales se puede destacar las Normas ISO/IEC 27037:2012, principalmente como la forma mediante la cual se deberá manejar la evidencia digital y medidas de seguridad en cuanto a los sistemas informáticos, así mismo se analizó el Código Orgánico Integral Penal, a fin de determinar los elementos constitutivos de los diferentes tipos penales los cuales trabajen con delitos informáticos, además de destacar lo singularizado por la Ley de Protección de Datos Personales la cual protege de manera directa al usuario de un sistema informático y además evita que este sufra alguna vulneración a su información personal, quedando de tal manera abarcado todo el contexto jurídico que nos encontramos para la tipificación, sanción y procedimiento mediante el cual se ejecutan los delitos informáticos y cuál es su grado de afectación de conformidad al bien jurídico que protegen

Ahora bien, esta información es vulnerada por delitos informáticos los cuales se tratan de utilizar medios electrónicos o informáticos, computadoras, teléfonos celulares, Tablet y cualquier otro dispositivo que tenga conexión a internet, estos delitos son propiciados por personas mal intencionadas que tratan de confundir a los clientes mediante casos relevantes como falsas identidades, filtro de información de las redes sociales, extorción por parte de estos individuos que solo buscan obtener información para poder causar robos de información sumamente valiosa y delicada de los clientes o usuarios de entidades financieras.

En cuanto al estudio comparado analizado al poder destacar principalmente la finalidad que mantiene el derecho penal dentro de lo que corresponde a la doctrina y la relativa novedad de los delitos informáticos es más que claro que existe vulnerabilidad en la protección de la información de los usuarios no solo en el sistema financiero, sino que también las afectaciones a sus bienes jurídicos abarcan mucho más allá de los económico

cayendo en delitos los cuales van en crecida, es evidente que la legislación mexicana confiere un óptimo plan de trabajo oportuno en materia de ciberseguridad informática y busca el trabajar con respaldo de las leyes para evitar que se afecten los bienes jurídicos protegidos.

7.1.1. Objetivos específicos

En el trabajo de integración curricular, se han planteado cuatro objetivos específicos, los cuales se listan a continuación:

4.12.1.1. Realizar un análisis en la legislación ecuatoriana respecto los delitos informáticos y vulnerabilidades de información.

En base al primer objetivo específico que se ha planteado, la legislación ecuatoriana aborda los delitos informáticos y la vulnerabilidad de la información se encuentra principalmente en el Código Orgánico Integral Penal (COIP) y otras leyes relacionadas con la protección de datos y la ciberseguridad. Esto lo hacemos conocer en el marco teórico donde se proporcionó una visión general de las principales disposiciones legales en Ecuador en este ámbito, que las vamos a citar a continuación:

Revelación ilegal de base de datos (Art. 229): El primero de los ciberdelitos tipificados y sancionados en el Código Orgánico Integral Penal, en cuanto a la persona que lo comete es independiente del cargo que ejecute siendo esta natural o jurídica, con el verbo rector de "revelar" y el objeto relacionado a "información registrada, contenida en ficheros, archivos, base de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones"; buscando la finalidad para que se constituya delito el "materializar voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas", tipifica una pena de privación de 1 a 3 años, y en caso de que este delito sea cometido por un servidor, empleado o empleada bancaria interno o

externo o de cualquier institución de la economía popular y solidaria esta pena llegara a ser de 3 a 5 años de privación de la libertad.

Interceptación ilegal de datos (Art. 230): El sujeto activo de esta infracción será cualquier persona, se mantiene una pena privativa de la libertad de 3 a 5 años de privación de la libertad y este delito mantiene causales para su comisión estando todas relacionadas de manera directa en la intervención de los datos que mantenga una determinada empresa o persona a través del uso de las Tics, en este tipo de delitos podemos presenciar la existencia directa de la intención de causar el daño a la posible víctima y por consiguiente acceder a la información que esta mantenga.

Transferencia electrónica de activo patrimonial (Art. 231): En este caso como sujeto activo de la comisión de este tipo penal nos encontramos directamente a cualquier persona que realice con el ánimo de un lucro el alterar, modificar o manipular el funcionamiento de un programa o sistema informático y telemático con el afán de procurarse una transferencia o transacción no permitida, dentro de este caso nos encontramos a una pena privativa de la libertad de 3 a 5 años; para este tipo penal no encontramos pena superior en el caso de que sea cometida de manera directa por un funcionario, servidor o trabajador de determinada institución bancaria por lo que es independiente del cargo que ejecute.

Ataque a la integridad de los sistemas informáticos (Art. 232): Para este tipo penal nos encontramos nuevamente como sujeto activo cualquier persona con los verbos rectores claros de destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento o comportamiento no deseado, suprimir total o parcial el contenido digital de los sistemas informáticos, encontraremos una pena privativa de la libertad de 3 a 5 años, manteniéndose esta pena en el caso de que se busque el diseño, desarrollo, programación, adquisición, envió, introducción, ejecución, venta o distribución dispositivos o programas

maliciosos; para este verbo rector nos encontramos con una mejora en la pena únicamente si la afectación se conlleva ante los servicios públicos que pasara a ser de 5 a 7 años.

Delitos contra la información pública reservada legalmente (Art. 233): Para este tipo penal como sujeto activo se encuentra cualquier persona, en este caso el verbo rector para este tipo penal nos encontramos con el destruir o inutilizar, en ese sentido es bastante claro, el objeto del delito versa sobre la información clasificada declarada de esa manera de conformidad a la ley, mantiene una pena privativa de la libertad de 5 a 7 años, dentro de este tipo penal, con diferente sujeto activo, siendo en este caso un servidor público, que obtenga esta información mantiene una pena privativa de la libertad de 1 a 3 años, es decir mucho menor a la que recibe la persona que destruya la información, finalmente en el caso de que esta información comprometa la seguridad integral del estado este delito será sancionado con una pena privativa de la libertad de 7 a 10 años, por lo que al ver los intereses del Estado comprometidos de por medio la sanción es más severa.

Ley Orgánica de Datos Personales (LOPD):

Esta ley regula el tratamiento de datos personales y la protección de la privacidad en Ecuador. Si bien no trata directamente delitos informáticos, establece normas estrictas sobre la recopilación, almacenamiento y uso de datos personales.

Así mismo en base a las encuestas y entrevistas realizadas en la pregunta número 5 se evidenció que el 93% de los encuestados están de acuerdo, es importante destacar que la regulación legal en este ámbito puede evolucionar y cambiar con el tiempo. Por lo tanto, es fundamental consultar las leyes y regulaciones más actualizadas y, si es necesario, obtener asesoramiento legal de expertos en la materia.

4.12.1.2. Determinar procesos que contengan, normas y políticas que nos ayuden a regular la vulnerabilidad de la información de los usuarios.

Para regular la vulnerabilidad de la información de los usuarios, es esencial implementar una serie de procesos, normas y políticas que promuevan la seguridad cibernética y la protección de datos en el contexto digital. Principalmente se puede buscar el trabajar varios puntos en concreto como lo son el identificar las posibles amenazas y vulnerabilidades que podrían afectar la seguridad de la información de los usuarios; con ello se procedería a realizar evaluaciones de riesgos para determinar qué activos de información son más valiosos y qué amenazas son más probables y perjudiciales. El estado ecuatoriano debería desarrollar políticas claras y detalladas que establezcan los principios y lineamientos para proteger la información y datos de los usuarios, así como también el definir reglas para el acceso a los sistemas, la gestión de contraseñas, la autenticación de usuarios y el uso adecuado de recursos tecnológicos.

Es evidente que existe escases en cuanto a los procesos los cuales toman las diferentes instituciones para poder asegurar y respaldar la información de sus usuarios, situación que ha generado inconformidad con los usuarios de estas plataformas, durante el desarrollo de las entrevistas hacia los abogados cuyo campo de trabajo se centra en las instituciones financieras podemos destacar en las preguntas tres y cuatro que estos coinciden en la necesidad por parte de las instituciones bancarias a fin de que se creen procesos mediante los cuales se pueda proteger la información de los usuarios de las diferentes plataformas digitales, así se puede garantizar de manera efectiva la seguridad de la información que por ley se encuentra categorizada como confidencial.

Así mismo la pregunta cuarta realizada en las entrevistas hacia los jueces y fiscales nos han determinado que existe una clara necesidad a la hora de establecer un proceso mediante el cual se pueda dar una correcta investigación a los ciberdelitos, es por ello que si se llega a configurar uno por la complejidad que se debe manejar a la hora de investigarlos, se

vulneran múltiples cadenas de custodia y por lo tanto la información puede sufrir graves alteraciones.

4.12.1.3. Realizar un estudio de derecho comparado respecto a los delitos informáticos.

En el presente objetivo específico aborda un estudio de derecho comparado analizando tres países España, México y Republica Dominicana en donde comprobamos que todas las legislaciones amparadas en la protección de los sistemas informáticos mantienen sus pros y contras, principalmente en donde no se llega apreciar un acuerdo entre las partes es cuando se trabaja en lo referente a las sanciones que les corresponden a las personas que infrinjan la normativa, con ello estas legislaciones nos dan a entender que han provocado múltiples vacíos entre ellas pero cada una mantiene su beneficio. Estas leyes establecen una serie de disposiciones para sancionar y prevenir delitos que involucran el uso de tecnologías de la información y la comunicación.

España por otro lado nos otorga a los ciberdelitos como una circunstancia agravante a las infracciones cometidas por parte de los investigados, de tal manera que esta legislacion ampara y protege a cabalidad los ideales de las diferentes empresas, otorgando un mecanismo adecuado para poder perseguir, sancionar y mitigar los daños ocasionados por una persona a la hora de provocar un ciberataque.

Finalmente, si hablamos de México es de los países que posee el espectro más amplio de conductas ciber-delictuales, de hecho, que se ha llegado a determinar la existencia de más de doscientos ciberdelitos. Entre ellos establecemos lo más importantes: “revelación de secretos, cracking, hacking, cyberbullying, spam, ciberpunk, acceso no autorizado a sistemas informáticos, entre otros” (Código Penal Federal México, 1999, pág. 120).

4.12.1.4. Elaborar lineamientos propositivos para refortalecer la seguridad de los sistemas informáticos tomando en consideración las medidas tomadas por otros estados.

En este objetivo se ve conveniente homologar ciertas normativas o leyes de otros países, y según el análisis que realizamos Uruguay tiene una legislación muy robusta para poder homologar a la nuestra es por ello que se plantea una homologación con esta legislación y así robustecer nuestra legislación ecuatoriana y que se defiendan el derecho a la privacidad de la información de los clientes de las entidades financieras. Gracias al desarrollo del derecho comparado se logró determinar que esta legislación es la más acertada para poder trabajar el tema en cuestión y por consiguiente con ello se pude progresar en mejor manera y magnitud con el evitar este tipo de delitos informáticos.

Si bien es cierto la aplicación de las normativas extranjeras en el país muchas veces implica limitaciones, principalmente por cuanto estas responden a la realidad social del país en el que pertenecen o responden, mientras que la realidad del Ecuador en ciertos aspectos se diferencia al contexto internacional; aun con ello existen parámetros que pueden llegar a ser aplicados para la realidad del país, tal como por ejemplo los términos y la forma de operar ante la existencia de un inminente peligro, es por ello que en base al derecho internacional, el Ecuador, podrá optar por afianzarse en las políticas de instituciones extranjeras.

De las preguntas número cuatro efectuada a los jueces y fiscales se puede observar que existe de manera clara la necesidad de establecer y crear procesos de investigación para la persecución de este tipo de infracciones y así evitar que estos delitos se queden en la impunidad.

De igual manera dentro de la pregunta cinco realizada a los jueces y fiscales llegan a varias soluciones para esta problemática planteada, parten por indicar que no necesariamente

se debe trabajar solo en la acción una vez que se comete el ilícito, sino que además se debe trabajar en la prevención del mismo, creando unidades especializadas por parte del Estado para actuar de manera inmediata ante la comisión del ilícito y por consiguiente evitar que estos delitos se sigan cometiendo por la mera inobservancia de los parámetros a seguir dentro de la institución.

7.2. Fundamentación jurídica de los lineamientos propositivos

Las vulnerabilidades de la información mediante los delitos informáticos en la actualidad se han vuelto algo común en nuestro medio, esto puede afectar directamente a los clientes ya que algunos de ellos desconocen los temas relacionados con el robo de información por medio de delitos informáticos, en este sentido es importante que los sistemas de justicia penal consideren que este tipo de delitos se deben investigar a profundidad y aplicar leyes que sean correspondientes.

Desde mi punto de vista jurídico, es evidente que la tecnología ha ido evolucionando día a día y los riegos de seguridad han ido decayendo, no solo está en el país sino a nivel mundial, por tal motivo es necesario el profundo análisis de las leyes actuales para la constancia de una armonía social.

En el marco del derecho comparado podemos constatar que el país con mayor rigurosidad en leyes que se aplican a este tipo de delitos es Mexico, el derecho a la privacidad y protección de datos nos ayuda a que las constitución y leyes de muchos países, incluyendo a este, reconocen el derecho a la privacidad y la protección de datos personales como derechos fundamentales. Esto establece una base legal para la implementación de medidas que garanticen la seguridad y confidencialidad de la información personal y financiera de los clientes bancarios.

Con el estudio de casos referente a las noticias se ha comprobado que son muchos los casos de vulneración de la información mediante delitos informáticos, y esto provoca mucho pánico en las personas que tienen sus ahorros en las entidades financieras puesto que pierden la seguridad de confiar su información.

De la misma manera podemos evitar que esta información sea vulnerada aplicando procesos que tengan normas y políticas que ayuden a mejorar la calidad de servicio en cada una de las entidades financieras.

Aplicando políticas de seguridad de la información estos se los desarrollará a nivel interno para luego comunicar estas políticas claras de seguridad de la información que establezcan los principios y objetivos de protección de datos y ciberseguridad en la organización.

Finalmente, también se pueden implementar evaluaciones de Riesgos y Amenazas las mismas que permitirán realizar evaluaciones regulares de riesgos y amenazas cibernéticas para identificar vulnerabilidades y tomar medidas preventivas.

Así mismo los clientes deben estar en constante capacitación continua a empleados sobre ciberseguridad y buenas prácticas para evitar ataques informáticos y prevenir el phishing.

Por lo tanto, se corrobora que mi propuesta de mejorar la seguridad del sistema penal ecuatoriano referente a la violación de la información de los usuarios tiene buena acogida en las muestras obtenidas en las encuestas realizadas.

8. Conclusiones

1. Ecuador es un país de constantes cambios que permite la investigación y sanción de la vulnerabilidad de la información por medio de los delitos informáticos actualmente, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones mantengan una dirección adecuada, con la capacitación de las personas especializadas dentro de un marco legal apropiado.
2. La tecnología avanza rápidamente a nivel mundial, pero a su vez ocasiona que aparezcan nuevas formas de delinquir, con la utilización por supuesto de los medios tecnológicos que por ser de libre acceso las personas terminan confiándose y agregando información en donde no deberían hacerlo.
3. De acuerdo a los datos obtenidos en las encuestas el 98% de los involucrados respondieron que la revelación de datos de una persona afecta directamente a su integridad, y además que la conducta delictiva de la persona que comete un delito informático es diferente a la que comete cualquier otro delito, la mayor parte de veces los ciberinfractores son personas con una instrucción académica relevante que utilizan los sistemas informáticos con gran facilidad y de la misma forma tratan de borrar todas las evidencias, de esta forma es difícil detectarlos.
4. Los Delitos Informáticos son parte del Derecho Penal, que van encaminados a la protección de las personas en razón del ejercicio y goce de sus derechos respaldados por la Constitución, y que se traduce como una norma legal sancionadora que debe ser respetada y garantizada, por lo que el 98% de los encuestados mencionan que deben existir sanciones rigurosas para las personas que cometen estos tipos de delito.
5. Elaborar propuesta jurídica que sustente la tipificación en el Código Orgánico Integral Penal, de la responsabilidad de los bancos e instituciones financieras por la

vulnerabilidad de la información de los clientes por medio de los delitos informáticos de apropiación ilícita de fondos de los que sus clientes son víctimas.

6. La ciberseguridad dentro de los sistemas informáticos pertenecientes a las Instituciones del Sector Económico, Popular y Solidario, deben reforzar sus medidas de seguridad en cuanto a los diferentes métodos para garantizar que no acceda personal no autorizado a los mismos.
7. El enfoque y trabajo por parte del país en cuanto a la Ciberseguridad no se han reforzado o no se ha profundizado en investigarlo de una manera efectiva, lo que ha provocado que sean un objetivo relativamente sencillo a ojos de los posibles infractores, además que al no producirse una normativa especial ni para su investigación ni sanción, provoca la existencia de lagunas legales, en las cuales se respaldan los presuntos infractores y con lo cual recaen en la impunidad.

9. Recomendaciones

1. Incentivar a los profesionales del derecho para su formación sobre el tema de los Delitos Informáticos, dando a conocer las respectivas investigaciones dentro del plano legal, para lo cual el respectivo Foro de Abogados en conjunto con el Colegio de Abogados, deberá proponer un seminario para la capacitación a todas los profesionales del derecho.
2. En los casos de que sea víctima de un delito informático tiene que dar a conocer a la Fiscalía o a la Policía Nacional de tal forma que puedan proceder a las investigaciones pertinentes dando protección a los derechos de la persona afectada.
3. Para mantener una información protegida es necesario el asesoramiento de una persona con conocimientos informáticos que le puedan ayudar a que la información ingresada cuente con todo el respaldo y se mantenga de una forma reservada.
4. Deben existir maestrías en delitos informáticos ya que este delito necesita de una ardua investigación para detectarlo y si los profesionales del derecho no cuentan con una preparación adecuada será más difícil dar soluciones a las personas afectadas.
5. Procurar la concientización en la sociedad, advertencias en programas televisivos sobre el uso de la tecnología, de este modo se tomarán en cuenta las medidas necesarias para impedir que los hackers o crackers se infiltren en los sistemas informáticos protegidos.

9.1 Lineamiento propositivo

En la presente investigación del Trabajo de Integración Curricular, se realizó un análisis a las diferentes vulnerabilidades que pueden llegar a afrontar las diferentes instituciones dentro del sector económico, popular y solidario principalmente aquellas cooperativas llegando a verificar que las Instituciones Financieras pertenecientes a la Economía Popular y Solidaria no se ha trabajado de la mejor manera, pues no solamente emiten ninguna información referente a las medidas que han tomado para evitar los posibles ciberataques, sino que además, al no existir un proceso mediante los cuales se protejan de estos ataques su seguridad esto representa un peligro para los ciudadanos y usuarios de las plataformas virtuales.

Se plantean los siguientes lineamientos con finalidad de mejorar significativamente la investigación, sanción y más que nada la prevención de los posibles ataques y ciberdelitos que afecten la seguridad de los sistemas informáticos de las instituciones financieras que se encuentran dentro del sector de la Economía Popular y Solidaria:

- Llevar a cabo acciones en conjunto con la Policía Nacional y la Superintendencia de la Economía Popular y Solidaria en la creación de un plan de acción e intervención para la posible comisión de delitos informáticos dependiendo del riesgo que este represente y la afectación que pueda llegar a generar el ataque, como lo son claves de cierres emergentes, intervenciones a través de correos especiales y llaves maestras a fin de bloquear la información catalogada como reservada, para ello se propone que la policía trabaje para desarrollar esta tecnología.
- Promover mecanismos de capacitación, evaluación, hacking ético y establecer una Red Team con la finalidad de que los sistemas informáticos de las Instituciones financieras pertenecientes a la Economía Popular y

Solidaria sean constantemente evaluados en cuanto a su correcto funcionamiento; estas capacitaciones y evaluaciones se realizarán como mínimo dos veces al año y cuyos resultados se deberán informar de manera directa a la Superintendencia de Economía Popular y Solidaria.

- En base a lo analizado en el derecho comparado de las legislaciones de España, México y República Dominicana, extender la categoría de ciber-delitos como una circunstancia agravante para aquellos que no contemplen su tipificación como delitos autónomos.
- A partir de la información obtenida y debido a la falta de norma sugerir la creación de un proyecto de ley a tratarse dentro de la Asamblea Nacional orientado en medidas de seguridad a tomar dentro de las plataformas digitales de las instituciones bancarias que pertenecen a la Economía Popular y Solidaria.

10. Bibliografía

Administración Monetaria y Financiera, Junta Monetaria, (2018) Reglamento de la Seguridad Cibernética de la Información.

Aguilar, P.A. (2015). ¿Derecho Informático o Informática Jurídica? Facultad de Derecho, Universidad Autónoma de México UNAM.

Alarcon Caparros, V. (2024) ¿Qué leyes regulan la ciberseguridad en la Unión Europea y en España? https://www.signaturit.com/es/blog/que-leyes-regulan-la-ciberseguridad-en-la-union-europea-y-en-espana/.

Asamblea Nacional (2004) Ley Organica de Transparencia y Acceso a la Informacion Publica.

Banco de Guayaquil (2023) Reporte Integrado 2022 https://assets.ctfassets.net/jhuukrkt1w7q/7uCSzGAMLGdqRdFHXZzIoA/179037a23b2bebe52f7990f5443d4384/Reporte_Integrado_2022_BG.pdf

Banco de Loja (2024) Informe Anual 2023. https://www.bancodeloja.fin.ec/Portals/0/Nuestro%20Banco/Información%20Accionistas/Informes%20Anuales/2023/Memoria_Institucional_Anual_2023.pdf?ver=jT9nWHPmHC1I25DinG2Y6Q%3d%3d

Banco del Pacifico (2023) Memoria de Sostenibilidad 2022. https://www.bancodelpacifico.com/BancoPacifico/media/pdf/RSC/Memorias/Memoria-de-Sostenibilidad-2022.pdf

Cámara de Diputados del H. Congreso de la Unión (2009) Código Penal Federal

Centro nacional de Ciberseguridad Republica Dominicana (2021). Estrategia Nacional de Ciberseguridad. https://rm.coe.int/3148-1-1-3-dr-plan-de-accion-complementario-ciberdelito/168094e80b.

Condor Rosas, J.P. (2024). Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la República del Ecuador, Colombia, Chile y Argentina. Universidad Técnica de Ambato, Facultad de jurisprudencia y ciencias sociales.

Congreso Nacional (2007) Ley Nro. 53-07 sobre Crímenes y Delitos de Alta Tecnológica.

Contreras Fresneda, S. (2024) Los delitos informáticos en el Código Penal. https://www.dexiaabogados.com/blog/delitos-informaticos/#:~:text=El%20artículo%20264%20castiga%20con,informáticos%20o%20documentos%20electrónicos%20ajenos.

Council of Europe (2001). Convenio sobre la ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Cuauhtémoc Vélez Martínez, M.A. (s.f.) Seguridad Informática. https://www.iingen.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx.

EAD TRUST (s.f.) ISO 27037 Directrices de gestión de evidencias electrónicas. http://foroevidenciaselectronicas.org/iso-27037-directrices-de-gestion-de-evidencias-electronicas/#:~:text=La%20norma%20ISO%20%2F%20IEC%2027037%3A2012%20proporciona%20orientación%20para%20los,de%20datos%20con%20funciones%20similares.

Enríquez Herrera, J. V., & Alvarado Salinas, Y. C. (2015). Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano. *Sathiri*, *8*, 171. https://doi.org/10.32645/13906925.404.

Global Suite Solutions (2023) ¿Qué son las normas ISO? https://www.globalsuitesolutions.com/es/que-son-normas-iso/

Kaspersky (s.f.) Qué es el pharming y cómo protegerte. https://latam.kaspersky.com/resource-center/definitions/pharming.

Kaspersky (s.f.) ¿Qué es el registro de pulsaciones de teclas y keyloggers? https://latam.kaspersky.com/resource-center/definitions/keylogger.

Mendoza, M.A. (2015) ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Ochoa Arevalo, P.A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. file:///G:/scalle-artculo-3.pdf

OpenWebinars; Lucena, C. (2019) Qué es el hacking https://openwebinars.net/blog/que-es-el-hacking/

PÀEZ, Rivadeneira. Luis. (2013). PeritajeInformático. PASCALE, Eduardo. (2012). Descubriendo rastros Informáticos. REBOLLO, Lucrecia. (2010). Derechos Fundamentale y Protecciòn de Datos . TÈLLEZ, Josè. (2012). DelitosInformáticos y Proteccion Penal a la Intimidad. TORRES, Andreìna. (2013). La Seguridad Pùblica en Ecuador un concepto en Construcciòn. Quito. VALLEJO DELGADO, Vicente. (2012). El Delito Informático en la Legislaciòn Ecuatoriana. ZAMBRANO, Regina. Reyna. (2012). Delitos Informáticos comtemplados en la Ley Ecuatoriana. Primera Edicion.

Panda Security (2023) Tipos de cibercrimen. https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen/#:~:text=Hay%20tres%20categorías%20principales%20en,en%20función%20de%20la%20categoría.

Perez Bes, F. (2021) Codigo de Derecho de la Ciberseguridad.

Reunión Especializada de Ministerios Públicos del MERCOSUR (2016). Guía de obtención, preservación y tratamiento de evidencia digital. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf.

Sain, G. (s.f.). Evolución histórica de los delitos informáticos. Revista Pensamiento Penal.

Secretaria Nacional de la Administración Publica (2013) Acuerdo Nro. 166. Esquema Gubernamental de Seguridad de la Información (EGSI)

Servicio Ecuatoriano de Capacitación Profesional (2020) Política de Acceso a Redes y Servicios de Red

Signaturit Group. (2024) ¿Qué es el Reglamento eIDAS y cómo beneficia a las empresas? https://www.signaturit.com/es/blog/que-es-el-reglamento-eidas-y-como-beneficia-a-las-empresas/

Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses (s.f.) Instructivo para el manejo de indicios y/o evidencia digital. https://www.fiscalia.gob.ec/files/archivos%20AC/COIP%20073%20FGE/Area%20de%20Cadena%20de%20Custodia/4__Instructivo_para_el_manejo_de_indicios_y-o_evidencia_digital.pdf.

Superintendencia de la Economia Popular y Solidaria (2022) Norma de Control respecto a la seguridad de la información del sector financiero popular y solidario abajo control de la Superintendencia de economía popular y solidaria.

Trejo, C.A.; y Calderon Cisneros, J.T. (s.f.) Capitulo III.- El phishing como nueva modalidad de fraude en la era digital.

11. Anexos

Anexo 1: Gráfico de la encuesta y entrevista

UNIVERSIDAD NACIONAL DE LOJA
FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA
CARRERA DE DERECHO
ENCUESTA PARA ABOGADOS EN LIBRE EJERCICIO PROFESIONAL

Estimado Abogado (a):

Me encuentro desarrollando mi Trabajo de Integración Curricular titulado: "**Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario**". Por lo tanto, requiero de su **criterio jurídico** respecto a mi investigación. Le ruego se sirva contestar las siguientes interrogantes:

1. ¿Conoce usted la norma jurídica que regula los ciberdelitos y la información de los usuarios del sector financiero?
   SI ( ) NO ( )

2. ¿Considera necesario establecer, procesos que contengan normas y políticas en las entidades financieras, con la finalidad que se mantenga segura la información de los usuarios de la entidad?
   SI ( ) NO ( )

¿Porqué?

_____
_____

3. ¿Conoce usted si en las entidades financieras de la Economía Popular y Solidaria, mantienen reglas centradas en la ciberseguridad en cuanto a la información de sus usuarios para que ésta no sea vulnerada a través de un ciberataque?

   SI ( ) NO ( )

¿Por qué?

_____
_____

4. ¿Conoce usted si se ha efectuado algún ataque a los sistemas informáticos de cualquiera de las Instituciones Financieras?
   SI ( ) NO ( )

¿Por qué?

_____
_____

5. ¿Está de acuerdo con que se establezcan Lineamientos Propositivos centrados en la prevención, erradicación y control de los ciberataques contra los sistemas informáticos? SI ( )
NO ( )

¿Por qué?

_____

_____

GRACIAS POR SU COLABORACIÓN

Formato de entrevistas

Entrevista a abogados en entidades financieras

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA

Estimado entrevistado (a):

Resumen: Los avances tecnológicos y con ello la sociedad ha dado muchos saltos a lo largo del tiempo y a través de las diferentes herramientas y tecnologías que día a día se desarrollan se ha vuelto imposible el hecho que no se relacionen con la actualidad y sobre todo con el derecho, a lo largo del presente trabajo de investigación se realiza un muy pormenorizado análisis de los que respecta a los sistemas informáticos y sobre todo las vulnerabilidades que llega a presentar las plataformas de las diferentes instituciones bancarias, así como también la forma que estas mantienen para protegerse de cualquier ciberataque.

Me encuentro desarrollando mi Trabajo de Integración Curricular titulado: **"Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario".** Por lo tanto, requiero de su criterio jurídico respecto a mi investigación. Le ruego se sirva contestar las siguientes interrogantes:

1. Usted como funcionario de una entidad financiera y encargada de la defensa de los derechos de los funcionarios y clientes de esta entidad ¿Tiene conocimiento sobre vulnerabilidades de la información a los usuarios por medio de delitos informáticos en el ámbito financiero? ¿Cree usted que se debería el plazo de 72 horas de justificación de la legal tenencia de mercancía conferido por el Código Orgánico Integral Penal es necesario?
2. En caso de que se presente en la entidad financiera casos de vulnerabilidad de la información ¿Estaría de acuerdo que se sancione con una pena privativa de libertad de 5 a 7 años según el Código Orgánico Integral Penal (COIP) Art. 233 a las personas que destruya o inutilice información clasificada de conformidad con la ley?
3. ¿Considera necesario establecer, procesos que contengan normas y políticas en las entidades financieras, con la finalidad que se mantenga segura no se vulnere la información de los clientes o usuarios de la entidad?
4. ¿Conoce usted si en las entidades financieras, está suficientemente protegida la información de sus clientes o usuarios para que ésta no sea vulnerada?

5. ¿Está usted de acuerdo que se debería mejorar la seguridad del sistema penal ecuatoriano referente a la violación de la información de los usuarios dentro de las entidades financieras?

GRACIAS POR SU COLABORACIÓN

Entrevista a jueces y fiscales

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA

Estimado entrevistado (a):

Resumen: Los avances tecnológicos y con ello la sociedad ha dado muchos saltos a lo largo del tiempo y a través de las diferentes herramientas y tecnologías que día a día se desarrollan se ha vuelto imposible el hecho que no se relacionen con la actualidad y sobre todo con el derecho, a lo largo del presente trabajo de investigación se realiza un muy pormenorizado análisis de los que respecta a los sistemas informáticos y sobre todo las vulnerabilidades que llega a presentar las plataformas de las diferentes instituciones bancarias, así como también la forma que estas mantienen para protegerse de cualquier ciberataque.

Me encuentro desarrollando mi Trabajo de Integración Curricular titulado: **"Vulnerabilidad de la información a los usuarios basados en delitos informáticos en el sistema financiero popular y solidario".** Por lo tanto, requiero de su criterio jurídico respecto a mi investigación. Le ruego se sirva contestar las siguientes interrogantes:

1. ¿Qué tan común es que avoque conocimiento por un delito informático?
2. Para la recopilación de la evidencia ¿Qué lineamientos siguen?
3. ¿Considera usted que las sanciones estipuladas para los ciber-delitos son proporcionales a la conducta generada?
4. ¿Cuál considera usted que sería un buen procedimiento para la investigación de los ciberdelitos?
5. ¿Qué solución usted le daría al problema planteado?

¡GRACIAS POR SU COLABORACIÓN

Anexo 2: Caso número 1, noticia

Mintel pidió a Banco Pichincha informar sobre el grado de vulnerabilidad por ataque cibernético

La **ministra de Telecomunicaciones y de la Sociedad de la Información** (Mintel), Vianna Maino, acudió este 13 de octubre del 2021 al llamado de la Comisión de Desarrollo Económico de la **Asamblea Nacional**, que busca conocer las causas y consecuencias de la **inhabilitación** de los **servicios** bancarios del **Banco Pichincha**.

La funcionaria señaló que, el pasado 11 de octubre, después de que el Banco Pichincha informó que la falla en el acceso y prestación de los servicios se debió a un "incidente de ciberseguridad" detectado en sus sistemas informáticos, el **Mintel** le solicitó a la **Superintendencia de Bancos** y al gerente de la entidad bancaria se den a conocer el estado real del ataque cibernético y el grado de cumplimiento de las medidas de respuesta a dicho incidente.

Anexo 3: Caso número 2, noticia

EL COMERCIO

ÚLTIMA HORA ACTUALIDAD TENDENCIAS DEPORTES OPINIÓN VIDEO PODCASTS BLOGS

Actualidad / SEGURIDAD

25 de julio de 2022 00:00

3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020

La **investigación policial** duró 11 meses. Luego de rastrear información por **medios electrónicos** y hacer un análisis de redes digitales, la **Policía** detuvo a tres presuntos ciberdelincuentes que se dedicaban a estafar en línea.

Durante un operativo, las tres personas fueron aprehendidas la madrugada del 2 de junio pasado. Según las pesquisas, ellos habrían creado una **página web** y una plataforma de comercio electrónico por redes sociales falsas. Operaban desde **Pichincha y Manabí**.

Agentes a cargo de este caso **detallaron** que los sospechosos usaban esos medios digitales para promocionar y vender **artículos electrónicos** a bajos precios.

Las víctimas se contactaban con ellos para **adquirir esos artefactos** y les depositaban el dinero en cuentas bancarias. Tras recibir el dinero, los **presuntos ciberdelincuentes bloqueaban** el contacto con los afectados y jamás enviaban el artículo solicitado.

Los ataques de las **cibermafias son recurrentes en el país**. Un informe estadístico de la **Unidad de Ciberdelitos** de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado **3 183 delitos informáticos**. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1 851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650 investigaciones a escala nacional.

Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias con más casos.

Anexo 4: Certificado de aprobación por parte del director.

Universidad Nacional de Loja

1859

Sistema de Información Académico Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, **Reategui Cueva Gladys Beatriz**, director del Trabajo de Integración Curricular denominado **VULNERABILIDAD DE LA INFORMACIÓN A LOS USUARIOS BASADOS EN DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO POPULAR Y SOLIDARIO**, perteneciente al estudiante **JUAN EFREN JUMBO CONDOLO**, con cédula de identidad N° **1104802440**. Certifico que luego de haber dirigido el **Trabajo de Integración Curricular** se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Integración Curricular**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Integración Curricular del mencionado estudiante.

Loja, 22 de Agosto de 2023

GLADYS BEATRIZ REATEGUI CUEVA

Firmado digitalmente por GLADYS BEATRIZ REATEGUI CUEVA
Fecha: 2023.08.22 11:45:37 -05'00'

F) ----------

DIRECTOR DE TRABAJO DE INTEGRACIÓN CURRICULAR

Certificado TIC/TT.: UNL-2023-000485

1/1

Educamos para **Transformar**