DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS

TEMA: ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y DE TELECOMUNICACIONES EN EL ECUADOR BAJO LAS NUEVAS NORMAS JURIDICAS

AUTOR: LLANGARÍ SALAZAR, ANDRÉS MAURICIO

DIRECTOR: ING. ALULEMA FLORES, DARWIN OMAR MSC.

SANGOLQUÍ

2016

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y DE TELECOMUNICACIONES EN EL ECUADOR BAJO LAS NUEVAS NORMAS JURIDICAS"** realizado por el señor **LLANGARÍ SALAZAR ANDRES MAURICIO**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor **LLANGARÍ SALAZAR ANDRES MAURICIO** para que lo sustente públicamente.

Sangolquí, 01 de Febrero del 2016

ING. DARWIN OMAR ALULEMA FLORES MSC.

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

Yo, **ANDRÉS MAURICIO LLANGARÍ SALAZAR**, con cédula de identidad N° 0603034034, declaro que este trabajo de titulación **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y DE TELECOMUNICACIONES EN EL ECUADOR BAJO LAS NUEVAS NORMAS JURIDICAS"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 02 de Febrero del 2016

ANDRÉS MAURICIO LLANGARÍ SALAZAR

C.C. 0603034034

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, **ANDRÉS MAURICIO LLANGARÍ SALAZAR**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y DE TELECOMUNICACIONES EN EL ECUADOR BAJO LAS NUEVAS NORMAS JURIDICAS"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 02 de Febrero del 2016

ANDRÉS MAURICIO LLANGARÍ SALAZAR

C.C: 0603034034

DEDICATORIA

A Dios y a la santísima Virgen Dolorosa, por darme la fortaleza para que logre cumplir uno de los objetivos de mi vida.

A mis padres Ángel Fernando y Mariana de Jesús, ya que con su paciencia, apoyo y sobretodo sus buenos consejos han sabido guiarme para terminar mis estudios y convertirme en profesional.

También a mi abuelito Luis Salazar que no avanzo a mirarme como profesional, ya que se adelantó al encuentro con Dios.

AGRADECIMIENTO

En especial a mis padres, ya que con su apoyo, cariño y respaldo siempre estuvieron preocupados de mí durante toda mi vida y en especial en el desarrollo de este trabajo.

A mi director de proyecto, ya que supo guiarme y darme pautas para la culminación del proyecto.

A todos mis amigos y amigas, que de manera directa o indirecta me ayudaron durante todos los años de vida universitaria.

Como también a toda mi familia que siempre estuvo pendiente en la finalización del proyecto.

INDICE DE CONTENIDOS

INDICE DE CUADROS

INDICE DE FIGURAS

RESUMEN

El presente proyecto trata sobre el análisis de Delitos Informáticos y de Telecomunicaciones, en los nuevos cuerpos jurídicos existentes en la República del Ecuador. Además en este proyecto, se establecen generalidades de los Delitos Informáticos y telecomunicaciones, como base y guía para su correcta interpretación y comparación con las normativas jurídicas existentes. Igualmente se aborda cual es el propósito para realizar este tipo de delitos, como también la clasificación y que medios tecnológicos pueden ocupar para realizar estos actos ilícitos. Incluso cuales serían las características que deben poseer los delincuentes. Se realizara una investigación tecnológica para evitar esta clase de delitos. Consecuentemente se ejecutará un análisis de los artículos en donde se encuentren tipificados tanto delitos informáticos como de telecomunicaciones; en el desarrollo se toman las leyes vigentes de la república del Ecuador, estas normas jurídicas son el Código Orgánico Integral Penal publicada en Febrero de 2014 y la Ley Orgánica de Telecomunicaciones publicada en Febrero de 2015 . Después se elaborará una comparativa y ver si son aplicables las leyes nacionales en los distintos delitos que se pueden ejecutar dentro del país ya se en establecimientos públicos o privados. Finalmente se investiga que procedimientos o que propuestas tiene el estado nacional para garantizar la seguridad de la información en todas las instituciones públicas o privadas; así mismo si el país cuenta con organismos especializados o leyes que puedan ofrecer una debida protección a los diversos sistemas informáticos y de telecomunicaciones en caso de ser víctimas de estos delitos.

PALABRAS CLAVES:

- **DELITOS INFORMÁTICOS.**
- **DELITOS TELECOMUNICACIONES.**
- **CÓDIGO ORGÁNICO INTEGRAL PENAL.**
- **NORMATIVAS JURÍDICAS.**
- **SEGURIDAD INFORMÁTICA.**

ABSTRACT

This project deals with the analysis of Cybercrime and Telecommunications, the new existing legal bodies in the Republic of Ecuador. Also in this project, an overview of the Computer Crime and telecommunications are established as the basis and guide for correct interpretation and comparison with existing legal regulations. Also addressed is the purpose for this type of crime, as well as the classification and technological means can take to make these illegal acts. Even what they would be the characteristics that must have the criminals. technological research is carried out to avoid this kind of crime. Consequently an analysis of items where they are established in both telecommunications and computer crime will run; in developing the laws of the Republic of Ecuador is taken, these legal norms are the Code of Criminal Integral published in February 2014 and the Telecommunications Act published in February 2015. After a comparison be drawn and whether national laws are applicable in the various crimes that can run inside the country and public or private establishments in. Finally it is proposed procedures or national state to ensure information security in all public and private institutions under investigation; Likewise if the country has specialized agencies or laws that can provide adequate protection to the various computer and telecommunications systems if they are victims of these crimes.

KEYWORDS:

- **CYBERCRIME.**
- **CRIMES TELECOMMUNICATIONS.**
- **INTEGRAL CODE CRIMINAL PENAL.**
- **LEGAL REGULATIONS.**
- **INFORMATIC SECURITY.**

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Antecedentes.

Junto al avance de la tecnología informática y telecomunicaciones existe influencia en casi todas las áreas de la vida social, es así que ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos y de telecomunicaciones.

Las telecomunicaciones constituyen uno de los sectores de mayor desarrollo tecnológico en el mundo. Las nuevas tecnologías brindan enormes ventajas para las sociedades, pero también a través de éstas se pueden realizar diversos tipos de fraudes, los cuales afectan a usuarios, operadores de telecomunicaciones y proveedores de servicios del mundo, causando cuantiosas pérdidas económicas.

Una de las tecnologías que se pueden utilizar es por medio de Internet que permite el acceso para cometer delitos con mucha mayor movilidad y libertad, pues dificultan la ubicación e identificación del infractor, ya que no se cuenta con algún medio físico que evidencie el cometimiento del fraude y la identificación del infractor.

Estos delitos son difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas. Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos. Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución.

Varios delitos que se dan en Ecuador son en relación con la informática y las telecomunicaciones, como son la utilización de terminales de telecomunicaciones sin autorización de su titular, la mera posesión de medios destinados específicamente a suprimir o neutralizar cualquier dispositivo técnico de protección de programas de ordenador, el descubrimiento y revelación de secretos de empresa o datos de carácter personal, el

apoderamiento de documentos electrónicos, la interceptación de las telecomunicaciones, o la producción de daños en equipos o material informático.

Las nuevas tecnologías pueden utilizarse para cometer otras conductas, como amenazas, coacciones, injurias o calumnias, suplantación de la personalidad, defraudaciones, infracciones contra la propiedad intelectual (reproducción, plagio o distribución, con ánimo de lucro, de obras) o delitos contra la intimidad y la propia imagen.

La persecución de estos delitos puede resultar compleja, tanto la identificación y enjuiciamiento del infractor como la obtención y presentación de pruebas, por lo que es necesario contar con un especialista en estos casos.

En un informe publicado en el año 2011 por la Superintendencia de Telecomunicaciones (SUPERTEL), se presentan los delitos en telecomunicaciones más comunes en Ecuador. En la lista se encuentra la clonación de teléfonos celulares, Call back o llamada revertida, Fraude tercer país, By pass, Fraudes Telefónicos a través de los PBX entre los más cometidos en Ecuador.

Los factores de crecimiento de estos delitos son la evolución y el fácil acceso a la tecnología, el poco conocimiento de los usuarios respecto a los diferentes tipos de delitos, la generación de nuevas formas para burlar los métodos de control implementados.

1.2. Justificación.

En la actualidad el país se encuentra en vías de desarrollo tecnológico y con esto se ha dado paso también a la evolución de las telecomunicaciones conjuntamente con la gran herramienta que se tiene hoy en día denomina Internet; con lo que se ha visto la necesidad de investigar acerca de los diversos delitos informáticos y de telecomunicaciones que se dan en Ecuador, ya que en algunos casos no se puede juzgar a la persona que ha cometido estos ilícitos ya que no se consideran como delitos en la leyes de Ecuador y esto con lleva que pueden quedar en la impunidad algunos delitos.

Cabe mencionar algunos factores del crecimiento de los delitos en telecomunicaciones a considerar son los siguientes:

- La evolución de la tecnología y el fácil acceso a la misma representan oportunidades para cometer fraudes. También ocasionan vulnerabilidad en las redes de telecomunicaciones.
- El poco conocimiento de los usuarios respecto a los diferentes tipos de delitos en el sector de las telecomunicaciones los hace más vulnerables.
- Cuando se aplica un método efectivo para el control de un determinado fraude, los estafadores comienzan a generar nuevas formas para burlar los métodos de control y seguir cometiendo delitos.
- Muchas veces, se brinda un servicio de telecomunicaciones, sin un previo análisis de las vulnerabilidades que éste podría causar a los usuarios y a las propias empresas.
- Actualmente, con el desarrollo de la tecnología, se ha desarrollado un sinnúmero de fraudes que afectan a las operadoras de telefonía fija y móvil, así como también a los usuarios.

Dentro de los delitos informáticos y de telecomunicaciones más importantes y que se dan con mayor frecuencia en las diversas formas antes mencionadas son:

- Suplantación de identidad.
- Fraudes en bancos y financieras.
- Fraudes en tarjetas de crédito.
- Llamadas internacionales.
- Mercancías no entregadas.
- Fraudes con subastas.
- Oportunidades de trabajos.

Todos estos delitos llevan a la necesidad de una legislación adecuada que sancione y tipifique este tipo de delitos que hará que los mismos no queden en la impunidad, permitiendo una adecuación de los nuevos sistemas legales. Lo que se pretenderá a través de esta investigación es analizar los diversos delitos que se cometen en Ecuador y que se puedan penalizar con los diversos artículos y leyes que existan.

1.3. Alcance

El proyecto propone un análisis a los cuerpos jurídicos del Ecuador en relación a los delitos informáticos y de telecomunicaciones, considerando las nuevas figuras jurídicas establecidas en el Código Orgánico Integral Penal y Ley Orgánica de Telecomunicaciones. Ya que en estas normativas jurídicas contemplan varios artículos que hacen referencia a delitos informáticos y de telecomunicaciones.

Se investiga de que se tratan y como se puede clasificar los diverso delitos informáticos y de telecomunicaciones.

Se realiza un análisis y comparación de cada uno de los cuerpos legales relacionados con los delitos informáticos y de telecomunicaciones. También de cómo se está estructurando planes para combatir los diversos delitos informáticos y de telecomunicaciones en un futuro y como estos pueden afectar al estado ecuatoriano.

1.4. Objetivos.

1.4.1. General

- Analizar los cuerpos jurídicos del Ecuador en relación a los delitos informáticos y de telecomunicaciones, considerando las nuevas figuras jurídicas establecidas en el Código Orgánico Integral Penal y Ley Orgánica de Telecomunicaciones.

1.4.2. Específicos

- Analizar la definición de los delitos informáticos y de telecomunicaciones.
- Estudiar los cuerpos legales que hacen referencia a delitos informáticos y de telecomunicaciones.
- Comparar los delitos informáticos y de telecomunicaciones con respecto a la legislación ecuatoriana.

1.5. Normativas tomadas por organismos internacionales.

Protocolo Mundial sobre Ciberseguridad y Ciberdelito

Durante el Foro para la Gobernanza de Internet celebrado en Egipto en 2009, Scholberg y Ghernaouti-Helie presentaron una propuesta de Protocolo Mundial sobre Ciberseguridad y Ciberdelito. El Artículo 1-5 se refiere al ciberdelito y recomienda la aplicación de disposiciones penales, de medidas contra el uso indebido de Internet por los terroristas, de medidas para la cooperación mundial y el intercambio de información, y de medidas en materia de derecho a la intimidad y derechos humanos. En junio de 2014, Scholberg presentó la 9ª edición de un proyecto de Tratado de las Naciones Unidas sobre un Tribunal Penal Internacional o Tribunal del Ciberespacio. El enfoque científico, que no se funda en un mandato oficial de las Naciones Unidas, destaca las dificultades relativas a la jurisdicción en el ciberespacio y elabora el concepto de tribunal internacional con jurisdicción limitada que es comparable al de la Corte Internacional de Justicia permanente. (Gercke, 2014)

Protección de la Infraestructura de Información Crítica en la Seguridad Cibernética (CIIP).

La CIIP es una derivación del concepto más ampliamente conocido como Protección de la Infraestructura Crítica (CIP), o la protección de las infraestructuras de energía, telecomunicaciones, suministro de agua, transporte, finanzas, salud y otras que permiten que funcione una nación.

Estas infraestructuras necesitan ser protegidas contra eventos accidentales y deliberados que no les permitirían operar correctamente y que impactarían severamente a la economía y al bienestar social de esa nación. (Burnett, Trend Micro Incorporated, & OEA, 2015)

Estas infraestructuras se han protegido contra los ataques físicos y el sabotaje durante muchas décadas. Sin embargo, varios países se dieron cuenta de que muchas de estas infraestructuras críticas también tenían algo en común: dependían en mayor o menor medida de las infraestructuras de

información (redes de telecomunicaciones y sistemas de cómputo, TIC). Y debido a esta dependencia nació la disciplina de Protección de la Infraestructura de Información Crítica (CIIP). Los gobiernos y la industria ha comprendido rápidamente esto, y ha surgido el concepto más amplio de seguridad cibernética que incluye la CIIP. (Burnett, Trend Micro Incorporated, & OEA, 2015)

El Internet se concibió intencionalmente para ser una red resistente, y fundamentalmente lo sigue siendo. Nunca fue diseñado para ser una infraestructura de información crítica vital en la que hoy se ha convertido, especialmente para las pequeñas empresas, cuya dependencia del correo electrónico, de los sitios web, del acceso a otros recursos en línea se incrementa cada día. El impacto de una pérdida seria del acceso a Internet durante un periodo prolongado es incalculable debido a la complejidad de nuestras dependencias. (Burnett, Trend Micro Incorporated, & OEA, 2015)

Por lo tanto, es esencial que los gobiernos trabajen muy de cerca con el sector privado, a menudo en Asociaciones Públicas-Privadas (PPPs) para ayudar a enfrentar las amenazas para estas Infraestructuras de Información Críticas (CCIs) y hallar soluciones.

Actualmente, un mayor número de estos sistemas se están computarizando con controles de comunicación remotos, y casi siempre están conectados a Internet de alguna forma. Eso significa que deben protegerse contra el mismo malware y contra las explotaciones que pueden afectar a los sistemas de cómputo de los hogares y de las pequeñas empresas. Sólo hay que imaginar una interrupción prolongada de Internet que no sólo lo privaría de su ancho de banda, sino que también detendría la estación encargada de bombear agua, el sistema que genera la electricidad, el centro de logística para distribuir materia prima a las fábricas de alimentos y supermercados, el oleoducto que lleva el combustible a las refinerías y a las gasolineras; la pesadilla sería interminable.

CAPÍTULO II

2. DELITOS INFORMÁTICOS

2.1. Definición de Delitos Informáticos

El constante desarrollo tecnológico que tiene la sociedad, supone una evolución en las formas de delinquir, dando lugar, a nuevos métodos de delitos tradicionales como también a través de medios digitales. Dado esta evolución se ha creado muchos sistemas interactivos online y de tratamientos en tiempo real. Estos sistemas se han visto la necesidad de implementar contraseñas identificativas de usuarios para controlar y restringir el acceso a los datos. (Informático, s.f.).

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto.

Según Davara Rodríguez, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Según Carlos Sarzana, cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo.

Según Jimena Leiva, toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma. (Acurio del Pino D. S.)

Según Julio Téllez Valdez, las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. (Acurio del Pino D. S.)

Partiendo de esta compleja situación y tomando como referencia el “Convenio de Ciberdelincuencia del Consejo de Europa”, se puede definir los delitos informáticos como: “los actos dirigidos contra la confidencialidad, la

integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

Las características principales de los delitos informáticos son:

- Sólo una determinada cantidad de personas pueden llegar a cometerlos.
- El sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
- Provocan pérdidas económicas.
- Son muchos los casos y pocas las denuncias.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Tienden a proliferar, por lo que se requiere su urgente regulación legal.
- Delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- "Actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos." (Informático, s.f.)
- "Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución." (Informático, s.f.)

2.2. Propósitos de los delitos informáticos

Los propósitos que tienen los delitos informáticos son de analizar posibles amenazas y vulnerabilidades dentro de sistemas informáticos, como también tener control de acceso a la información.

2.2.1 Amenaza

"Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema." (Roldán, s.f.)

Una amenaza se representa por medio de una persona, evento, circunstancia o idea maliciosa, que pueda provocar un daño en caso de que se viole la seguridad, y pueden provenir de diferentes fuentes:

De humanos: Se refiere a aquellas amenazas que surgen debido a alguna acción humana, es decir, falta de conocimientos por parte de los usuarios para manejar los equipos, descuido de la información y daños provocados por todo tipo de atacantes.

De hardware: Son todas aquellas fallas físicas que puedan sufrir los equipos y dispositivos. Problemas en el suministro de energía, variación de voltaje, bajo rendimiento, deterioro de los equipos o defectos de fábrica.

De red: Son aquellas amenazas que tienen que ver con la red, por ejemplo congestionamiento o tráfico en la red, falla en la disponibilidad de la red o desconexión del canal.

De software: Tienen que ver con problemas lógicos en los sistemas, es decir que el software falle o no funcione correctamente, que exista código malicioso en los equipos, intrusión de virus o gusanos, etcétera.

2.2.2 Vulnerabilidad

“Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.” (Roldán, s.f.)

Las vulnerabilidades son muy variadas y al igual que las amenazas poseen una clasificación de acuerdo a su origen:

De hardware: Al igual que las amenazas, las vulnerabilidades de hardware tienen que ver son los dispositivos y equipos. En este caso son consideraciones no tomadas en cuenta para el buen funcionamiento, por ejemplo no darle mantenimiento constante al hardware, no verificar que el equipo que se compra cuente con los requerimientos necesarios, entre otros.

De software: Las fallas en los sistemas o debilidades en los programas instalados son ejemplos de este tipo de vulnerabilidades. Como su nombre lo

dice, se refiere a aquellas relacionadas con el software como errores de programación, o que los protocolos de comunicación carezcan de seguridad.

De red: Son todas aquellas vulnerabilidades existentes en la conexión de equipos, por ejemplo si no existe un control que permita limitar el acceso, se puede penetrar al sistema por medio de la red. También abarca las fallas en la estructura del cableado y el no seguir los estándares recomendados para realizarlo.

Humana: Del mismo modo que las amenazas humanas, las vulnerabilidades tienen que ver con las acciones de las personas, por ejemplo ser vulnerable a la ingeniería social, no capacitar al personal como se debe, colocar contraseñas en lugares visibles, entre otras.

2.2.3 Control de Acceso

"Es la habilidad de permitir o negar el acceso a una entidad. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, lógicos y digitales". (ALEGSA.COM.AR, s.f.)

Se necesita autenticar la identidad de los usuarios o grupos y autorizar el acceso a datos o recursos. Los controles de accesos son necesarios para proteger la confidencialidad, integridad y disponibilidad de los objetos, y por extensión de la información que contienen, pues permiten que los usuarios autorizados accedan solo a los recursos que ellos quieren para realizar sus tareas.

2.2.3.1 Objetivos del control de acceso

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización. Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas. Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

El control de acceso consta de tres pasos. Estos pasos son la identificación, autenticación y autorización. Con el uso de estos tres principios un administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema.

2.2.3.2 Identificación

Es la forma en que una entidad se presenta ante un sistema. La forma más común de identificación es el nombre de usuario o login.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Para el caso de sistemas o procesos los mecanismos de identificación que se pueden utilizar son: Nombre del equipo, Dirección MAC, Dirección IP. (Seguridad Informatica, 2011)

2.2.3.3 Autenticación

Proceso en Virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

La autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. Autenticación es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así. Lo más común es solicitar una contraseña o password. (Seguridad Informatica, 2011)

2.2.3.4 Autorización

El proceso de autorización es utilizado para decidir si una persona, programa o dispositivo tiene acceso a: archivos, datos, funcionalidad o servicio específico. Este proceso determinar que tiene permitido hacer.

Es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos usuarios a los que se les ha concedido autorización para ello. Los recursos incluyen archivos y otros objetos de dato, programas, dispositivos y funcionalidades provistas por aplicaciones. (Seguridad Informatica, 2011)

2.3. Delincuencia y criminalidad informática

2.3.1. Sujeto Activo

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Los delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. (Acurio del Pino S.)

Dentro de los sujetos activos se puede mencionar a los diversos tipos de que existen como son ***Hackers, Crackers, Lamers, Newbie, Script Kiddie***

2.3.1.1. Hackers

Un Hacker en plenitud tiene la capacidad de dominar en un buen porcentaje varios aspectos como: lenguajes de programación, manipulación

de hadware & software, telecomunicaciones, como también es alguien que descubre las debilidades de un computador o de una red informática. Todo esto lo pueden realizar para lucrarse, darse a conocer, por motivación, pasatiempo o para realizar actividades sin fines lucrativos.

La subcultura que se ha desarrollado en torno a los hackers a menudo se refiere a la cultura underground de computadoras, pero ahora es una comunidad abierta.

Los hackers han evolucionado de ser grupos clandestinos a ser comunidades con identidad bien definida. De acuerdo a los objetivos que un hacker tiene y, para identificar las ideas con las que comulgan, se clasifican principalmente en: hackers de sombrero negro, de sombrero gris, de sombrero blanco. (Wikepedia, s.f.)

2.3.1.1.1. Sombrero blanco

Un hacker de sombrero blanco rompe la seguridad por razones no maliciosas, quizás para poner a prueba la seguridad de su propio sistema o mientras trabaja para una compañía de software que fabrica software de seguridad. El término sombrero blanco en la jerga de Internet se refiere a un hacker ético. Esta clasificación también incluye a personas que llevan a cabo pruebas de penetración y evaluaciones de vulnerabilidad dentro de un acuerdo contractual. El Consejo Internacional de Consultores de Comercio Electrónico (EC-Council), ha desarrollado certificaciones, cursos, clases y capacitaciones en línea cubriendo toda la esfera del hacker ético. Además existen certificaciones como CPEH Certified Professional Ethical Hacker y CPTE Certified Penetration Testing Engineer de Mile2, que cuentan con acreditaciones de la Agencia Nacional de Seguridad de los Estados Unidos (NSA) y de la Iniciativa Nacional para los Estudios y Carreras en Ciberseguridad de los Estados Unidos (NICCS). (Wikepedia, s.f.)

2.3.1.1.2. Sombrero negro

Un hacker de sombrero negro es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal, los

hackers de sombrero negro son la personificación de todo lo que el público teme de un criminal informático.

Los hackers de sombrero negro entran a redes seguras para destruir los datos o hacerlas inutilizables para aquellos que tengan acceso autorizado. (Wikepedia, s.f.)

2.3.1.1.3. Sombrero gris

Un hacker de sombrero gris es una combinación de hacker de sombrero negro con el de sombrero blanco. Un hacker de sombrero gris puede navegar por la Internet y violar un sistema informático con el único propósito de notificar al administrador que su sistema ha sido vulnerado, por ejemplo luego se ofrecerá para reparar el sistema que él mismo violó, por un módico precio. (Wikepedia, s.f.)

2.3.1.2. Craker

Al igual que el hacker, el cracker es también un apasionado del mundo informático. La principal diferencia consiste en que la finalidad del cracker es dañar sistemas y ordenadores. Tal como su propio nombre indica, el significado de cracker en inglés es "rompedor", su objetivo es el de romper y producir el mayor daño posible. (Sarasola, s.f.)

“Para el hacker, el cracker no merece ningún respeto ya que no ayudan ni a mejorar programas ni contribuyen a ningún avance en ese sentido.” (Sarasola, s.f.)

Desde distintos ámbitos se ha confundido el término hacker con el de cracker, y los principales acusados de ataques a sistemas informáticos se han denominado hackers en lugar de crakers.

La acción de crackear requiere un mínimo conocimiento de la forma en que el programa se protege. Por lo general, los programas tienen la protección o activación por número de serie. Otros hacen la activación por medio de artimañas, en las cuales utilizan técnicas como registro vía web, vía algún mecanismo físico (activación por hardware) o por algún archivo de registro. El crackeo de software es una acción ilegal en prácticamente todo el mundo, ya

que para lograrlo es necesario utilizar la ingeniería inversa y sirve para elimina limitaciones que fueron impuestas por el autor para evitar su copia ilegal. (Sarasola, s.f.)

Otras veces se trata de dar más prestaciones de las que la versión del programa proporciona, como eliminar las ventanas que piden el registro del programa en programas shareware.

2.3.1.3. Lammers

Un lammer es una persona que presume tener varias habilidades como las de un hacker, lo cual es falso. Este tipo de personas son inmaduras, poco sociables, tienen poco conocimiento sobre informática y es un aficionado a un tema. Por lo regular las acciones que realizan este tipo de personas es el de visitar varios sitios web, descargan programas que ya han realizado personas conocimiento y luego generan ataques con este software. (Hacker, Cracker, Lammer, Newbie., 2009)

Estas personas no tienen conocimiento sobre el verdadero hack de una computadora por lo que al utilizar herramientas de hacking se sienten superiores a los programadores sintiéndose mejores que los demás. El riesgo que se corre con este tipo de personas es que intenten utilizar algún tipo de herramienta que haga vulnerable la seguridad de nuestro sistema de cómputo, tan solo por diversión o por probar una herramienta nueva. (Hacker, Cracker, Lammer, Newbie., 2009)

2.3.1.4. Newbie

Una persona newbie es aquel que está comenzando en el tema de hacking, es decir es un hacker novato. Tratan de ingresar a sistemas con muchos tropiezos en el camino esto lo hacen para aprender técnicas. Preguntan a expertos o hackers experimentados luego tratan de realizar las hazañas de otros. Estas personas son más precavidas y cautelosas que los lammers, aprenden métodos de hacking, utilizan el conocimiento para aprender, llegan a apasionarse por la informática para llegar a ser un hacker. (Hacker, Cracker, Lammer, Newbie., 2009)

2.3.1.5. Script Kiddie

Denominados Skid kiddie o Script kiddie, son el último eslabón de los clanes de la Red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack en su estado puro. En realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los ficheros de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propio ordenador. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking

2.3.2. Sujeto Pasivo

El sujeto pasivo es la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra". (Acurio del Pino S.)

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento. (Acurio del Pino S.)

En el mismo sentido, se puede decir que con:

- “Alertas a las potenciales víctimas, para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática.” (Acurio del Pino S.)
- Una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas. Se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más. (Acurio del Pino S.)
- Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos. (Acurio del Pino S.)

2.4. Tipos y Clasificación de Delitos Informáticos

Tomando como referencia al estadounidense Don B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas se ha clasificado a los delitos informáticos de la siguiente manera.

2.4.1 Fraudes

2.4.1.1 Datos falsos o engañosos (Data diddling)

Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. (Pino)

2.4.1.2 Manipulación de programas o los “caballos de troya” (Troya Horses)

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. (Pino)

2.4.1.3 Técnica del salami (Salami Technique/Rounching Down)

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta el dinero de muchas cuentas corrientes. (Pino)

2.4.1.4 Falsificaciones informáticas

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos. (Pino)

2.4.1.5 Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito. (Pino)

2.4.1.6 Pishing

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar. (Pino)

2.4.2 Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

2.4.2.1 Bombas lógicas (Logic Bombs)

Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba. (Pino)

2.4.2.2 Gusanos

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. (Pino)

2.4.2.3 Virus informáticos y malware

Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método

del Caballo de Troya. Han sido definidos como “pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autoreproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar” (Pino)

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos. (Pino)

2.4.2.4 Ciberterrorismo

Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común. (Pino)

2.4.2.5 Ataques de denegación de servicio

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas. (Pino)

2.4.3 Espionaje informático y el robo o hurto de software

2.4.3.1 Fuga de datos (Data Leakage)

También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. La forma más sencilla de proteger la información confidencial es la criptografía. (Pino)

2.4.4 Robo de servicios

2.4.4.1 Hurto del tiempo del computador.

Consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios. (Pino)

2.4.4.2 Parasitismo informático (Piggybacking) y suplantación de personalidad (Impersonation)

Figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

2.4.5 Acceso no autorizado a servicios informáticos

2.4.5.1 Puertas falsas (Trap Doors)

Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo

fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante. (Pino)

2.4.5.2 Llave maestra (Superzapping)

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación. (Pino)

2.5. Investigación tecnológica de los delitos informáticos

Consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general económico, causando un efecto negativo en la seguridad del sistema, que luego implica directamente en los trabajadores de la organización. (YADERSY, 2014)

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde el punto de vista del profesional de seguridad, se debe aprovechar esas habilidades para entender y estudiar la forma en que los atacantes llevan a cabo un ataque. (YADERSY, 2014)

Son cinco las etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:

2.5.1. Etapa 1: Reconnaissance (Reconocimiento)

Esta etapa involucra la obtención de información con respecto a una viable víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo.

Ejemplo el atacante sabe de la existencia de un amigo de la víctima y sabe que no tiene una red social en donde la victima está, por ejemplo Facebook, además sabe que no se han hablado desde hace tiempo o está lejos, pues el atacante hace una suplantación de identidad y obtiene información. (YADERSY, 2014)

Algunas de las técnicas utilizadas en este primer paso son la:

- Ingeniería Social, es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente, puede engañar fácilmente a un usuario en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y contraseñas. (YADERSY, 2014)

- Para evitar situaciones de Ingeniería Social es conveniente tener en cuenta estas recomendaciones:

Tener servicio técnico propio o de confianza.

Enseñar a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y derriben la inquietud a los responsables que tenga competencia para dar esa información.

Asegurarse que las personas que llaman por teléfono son quien dice ser. Por ejemplo si la persona que llama se identifica como proveedor de Internet lo mejor es cortar y devolver la llamada a forma de confirmación. (YADERSY, 2014)

- El Sniffing, es un programa informático que registra toda la información que envían los periféricos de un ordenador, así como, toda actividad realizada por este equipo informático. Es decir, es un pequeño programa que cuenta con la capacidad de capturar y registrar toda la transferencia de archivos de un ordenador. Son programas utilizados por administradores de redes para gestionar dichas redes de manera eficiente. Viéndolo desde este punto de vista, podemos decir que un Sniffer es un programa diseñado para capturar datos dentro de una red informática. (YADERSY, 2014)

En pocas palabras, un Sniffer es un programa que rastrea toda la información que transita a través de una red. (YADERSY, 2014)

2.5.2. Etapa 2: Scanning (Exploración)

En esta segunda etapa se utiliza la información obtenida en la etapa 1 para explorar el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el: Port mappers, network scanners, port scanners, y vulnerability Network mappers, que es un libre código abierto (licencia) de utilidad para la detección de red y auditoría de seguridad. Muchos sistemas y administradores de red también les resultan útiles para tareas como inventario de la red, la gestión de los horarios de servicio de actualización y supervisión de host o tiempo de servicio. (YADERSY, 2014)

Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra los ejércitos individuales. Se ejecuta en todos los principales sistemas operativos de ordenador, y los paquetes oficiales binarios están disponibles para Linux, Windows y Mac OS X. (YADERSY, 2014)

Esta es la fase que el atacante realiza antes de la lanzar un ataque a la red (network). En el escaneo el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento (Fase 1) para identificar vulnerabilidades específicas. Por ejemplo, si en la Fase 1 el atacante descubrió que su objetivo o su víctima usa el sistema operativo Windows XP entonces el buscara vulnerabilidades específicas que tenga ese sistema operativo para saber por dónde atacarlo. (YADERSY, 2014)

También hace un escaneo de puertos para ver cuáles son los puertos abiertos para saber por cual puerto va entrar y usa herramientas automatizadas para escanear la red y los host en busca de más vulnerabilidades que le permitan el acceso al sistema. (YADERSY, 2014)

2.5.3. Etapa 3: Gaining Access (Obtener acceso)

Es la instancia donde comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración. (YADERSY, 2014)

Algunas de las técnicas que el atacante puede utilizar son ataques de:

- Buffer Overflow, En seguridad informática y programación, un desbordamiento de buffer (del inglés buffer overflow o buffer overrun) es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer): Si dicha cantidad es superior a la capacidad preasignada, los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Esto constituye un fallo de programación. (YADERSY, 2014)
- Denial of Service (DoS), En seguridad informática, un ataque de prohibición de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Un ejemplo notable de este tipo de ataque se produjo el 27 de marzo de 2013, cuando un ataque de una empresa a otra inundó la red de spam (correo basura) provocando una disminución de la velocidad generalizada de Internet e incluso llegó a afectar a puntos clave como el nodo central de Londres. (YADERSY, 2014)
- Confidencialidad. Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. (YADERSY, 2014)
- Disponibilidad. En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del

sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información. (YADERSY, 2014)

2.5.4. Etapa 4: Maintaining Access (Mantener el acceso)

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos. (YADERSY, 2014)

Una vez el atacante gana acceso al sistema objetivo (etapa 3) su prioridad es mantener el acceso que gano en el sistema. En esta fase el atacante usa sus recursos y los del sistema y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados Sniffer para capturar todo el tráfico de la red, incluyendo sesiones de telnet y FTP (protocolo de transferencia de archivos). (YADERSY, 2014)

En esta fase el atacante puede tener la habilidad de subir, bajar y alterar programas y data. En esta fase el atacante quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los caballos de Troya (Trojans) para transferir nombres de usuarios, contraseñas e incluso información de tarjetas de crédito almacenada en el sistema. (YADERSY, 2014)

2.5.5. Etapa 5: Covering Tracks (Borrar huellas)

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). (YADERSY, 2014)

Un ejemplo de ataque informáticos es el Sasser y Netsky, el gran golpe del niño genio. Con sólo 17 años el joven alemán Sven Jaschan se transformó

en toda una celebridad mundial en 2004, cuando sus dos programas generaron estragos en Internet. Pese a que sus dos gusanos tenían comportamientos diferentes, las autoridades lograron encontrar similitudes en el código de ambos, llegando a rastrear a su creador. (YADERSY, 2014)

Sasser se diferenciaba porque en vez de propagarse vía e-mail (no eran necesarios usuarios para propagarse, lo hacía descargando un virus y buscar otras direcciones IP vulnerables a través de la red (como sistemas Windows 2000 y Windows Xp no actualizados), donde su principal “marca” era impedir que el equipo se apagar normalmente. Netsky, en tanto, se movía a través de los correos usando “parodias”, generando de paso ataques DDoS. Su propagación fue tal, que se llegó a considerar que el 25% de los ataques en el mundo tenían su procedencia. En lo legal, al no ser mayor de edad, Jaschan quedó en libertad, pese a los US$ 18.100 millones que generó en pérdidas. (YADERSY, 2014)

CAPÍTULO III

3. DELITOS DE TELECOMUNICACIONES

3.1. Definición de Delitos de telecomunicaciones

El delito en telecomunicaciones implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje. (mx, s.f.)

3.2. Propósitos de los delitos de telecomunicaciones

Los propósitos en telecomunicaciones se basan en los mismos que se dan en delitos informáticos, pero también se hace referencia en especial en fraudes ya que afecta a todos los operadores de telecomunicaciones y prestadores de servicios en sus ingresos. Diversas fuentes calculan que las compañías pierden cerca del 10% de sus ingresos por falta de herramientas tecnológicas y procedimientos para contralar el fraude y asegurar sus ingresos.

La movilidad es un motivo para que no se puedan detectar estos fraudes ya que a diferencia del cliente de servicio fijo (se lo puede ubicar), el del móvil es más propenso a no ser ubicado ya que este puede dar documentación falsa de sus datos personales y de esta manera esfumarse para no ser capturado en caso que no realice actos ilícitos (fraude).

3.3. Delincuencia y criminalidad de telecomunicaciones

3.3.1. Sujetos Activos en Telecomunicaciones.

Son las personas que adquirieron ciertas habilidades y que la mayoría de los delincuentes no poseen, los sujetos activos tienen habilidades para el manejo de sistemas en Telecomunicaciones y mayormente por su actividad laboral se encuentran en departamentos donde se dispone información de carácter privada, o bien son hábiles en el uso de los sistemas informáticos.

Al igual que en delitos informáticos también existen sujetos activos entre los cuales se encuentran: ***Copyhackers, Bucaneros, Phreaker.***

3.3.1.1. Copyhackers

Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año más de 25.000 millones de pesetas sólo en Europa. En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura. Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello " extraen " información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

3.3.1.2. Bucaneros

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos " Crackeados" pasan a denominarse " piratas informáticos ", el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

3.3.1.3. Phreaker

Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

3.3.2. Sujetos Pasivos en Telecomunicaciones.

Sujeto pasivo o víctima del delito es sobre el cual actúa el sujeto activo; de igual forma como lo es cuando se comenten delitos informáticos, en el caso de los "delitos en Telecomunicaciones " las víctimas pueden ser individuos, gobiernos o instituciones privadas, cuando usan sistemas de telecomunicaciones para la transmisión de datos.

El sujeto pasivo del delito que ocupa, es sumamente importante para el estudio de los delitos, ya que mediante él se conoce los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

3.4. Tipos y Clasificación de Delitos de telecomunicaciones

3.4.1. Clonación de teléfonos celulares

Es el fenómeno mediante el cual se copia del aire, el número telefónico y Equipment Serial Number (ESN, número de serie del equipo), para ser programados en otro aparato. Esto puede ser logrado gracias a un proceso de monitoreo o por medio de un laboratorio, cuando se lleva a reparar el celular. El aparato reprogramador o clon, al generar el tráfico telefónico, produce una factura al verdadero suscriptor del servicio. De esta manera, el aparato fraudulento utiliza el servicio sin pagar por él. (Supertel, 2011)

En otras ocasiones, cuando los teléfonos de los usuarios son robados o se extravían, los defraudadores toman el ESN directamente del equipo, el cual es válido hasta el momento de reporte por parte de la persona afectada a los operadores de servicio.

Además del cobro por llamadas efectuadas por el usuario fraudulento, el fraude de clonación en sistemas móviles puede causar la pérdida temporal del servicio al subscriptor y, eventualmente, la necesidad de programar el teléfono celular con un nuevo número.

Esta modalidad de fraude es muy usada por la delincuencia común y organizada con el fin de evitar el pago correspondiente a las llamadas realizadas y además evitar el seguimiento de las autoridades. (Supertel, 2011)

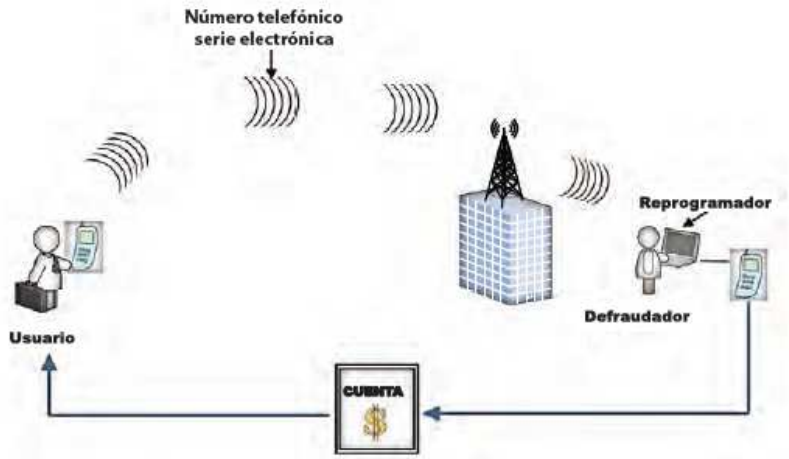

Figura 1.Fraude por clonación de celulares.

Fuente: *(Supertel, 2011)*

Los indicios de que un teléfono celular ha sido clonado pueden ser:

• Caídas frecuentes de conexión

• Dificultades para completar llamadas generadas

• Dificultades para llamar al buzón de mensajes

• Llamadas recibidas de números desconocidos, nacional e internacional

• Valores elevados en la factura (Supertel, 2011)

3.4.2. Call back o llamada revertida

Se denomina call back al procedimiento mediante el cual se revierte el origen del tráfico internacional, haciendo una llamada disparo" hacia un número predeterminado en el exterior. Esta llamada internacional no es contestada y, por tanto, no es cobrada. Un equipo al otro lado de la línea identifica y guarda el número desde el cual se hizo la llamada. Una vez que la persona que llamó cuelga, se le devuelve la comunicación con tono del país en el exterior y se gestiona como si fuera local. Existen tres pasos para el establecimiento en una llamada tipo call back, a continuación se los describe. (Supertel, 2011)

Paso No. 1

Desde Ecuador se realiza una llamada al exterior, a través de una operadora legalmente establecida en nuestro país; esta llamada no es contestada, por lo tanto, no es cobrada al usuario. Sin embargo, hay una tarifa de interconexión entre la operadora que cursa la llamada desde Ecuador hacia aquella en el exterior, la cual terminará la llamada hacia la empresa de call back. En el exterior, ésta registra el número con el que se llamó desde Ecuador. Cabe mencionar que la operadora internacional no sabe que está cursando la llamada hacia una empresa que realiza call back. (Supertel, 2011)

Figura 2. Establecimiento de call back paso 1.

Fuente: *(Supertel, 2011)*

Paso No. 2

La empresa de call back realiza una llamada revertida, marcando el número que sus equipos registraron, es decir, el número A, y se le da tono de marcado. En este caso, se tiene una tarifa b, que es de interconexión internacional desde el exterior hacia Ecuador, la que es mucho menor a la tarifa de interconexión desde Ecuador hacia el exterior (tarifa a). (Supertel, 2011)

Figura 3. Establecimiento de call back pasó 2.

Fuente: *(Supertel, 2011)*

Paso No. 3 (establecimiento del call back)

La tarifa c, que es la que se debe pagar por realizar la llamada como si se estuviera en el exterior, es determinada por la empresa que realiza la llamada revertida o call back, y cada país posee una tarifa diferente de acuerdo a la demanda que se tenga. Ésta es cancelada a través de tarjetas prepago o de páginas web, donde es normal que se oferten este tipo de llamadas.

En Ecuador, aproximadamente, en el año 1995, apareció este tipo de servicio de manera no autorizada; sin embargo, con la implementación del equipamiento adecuado en la central telefónica de tránsito internacional, se combatió esta clase de ilícito con eficacia. (Supertel, 2011)

Figura 4. Establecimiento Call Back pasó 3.

Fuente: *(Supertel, 2011)*

3.4.3. Fraude tercer país

Es el procedimiento mediante el cual el país X, que origina el tráfico telefónico, lo enruta hacia un país Z, que no es el destino final de la llamada. El país Z reenruta este tráfico hasta su último destino, el país Y. Debido a las diferencias tarifarias entre países, aquel que origina la llamada paga una tarifa más baja al dirigir la llamada primero hacia el país Z, para que desde ahí la comunicación termine en el tercer destino. Debido a esas diferencias de costos entre los Estados involucrados, el que origina el tráfico paga una tarifa de terminación más baja que el país de destino. A aquel que sirve de tránsito, generalmente, no se le paga nada. (Supertel, 2011)

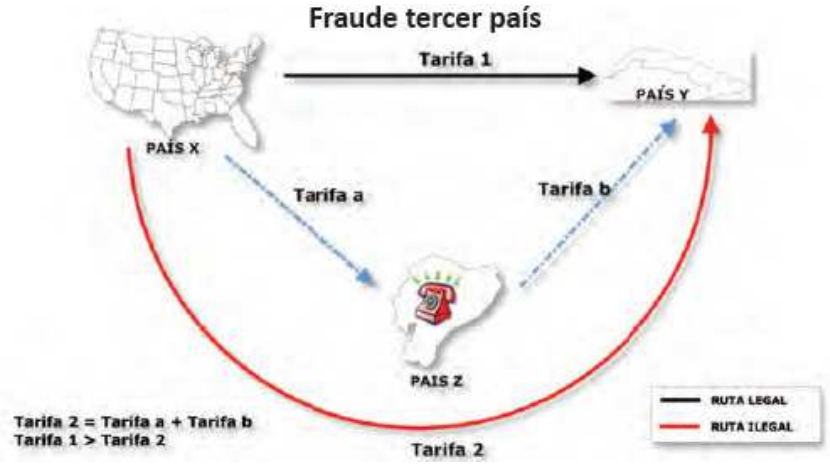

Figura 5. Fraude tercer País.

Fuente: *(Supertel, 2011)*

Este tipo de fraude se caracteriza por el destino atípico de las llamadas que generalmente son a países del África, de Medio Oriente (San Marino, Sierra Leona, Liberia, etc) y Cuba. Además el consumo telefónico es elevado y se generan llamadas las 24 horas del día. (Supertel, 2011)

3.4.4. Fraude en roaming

El fraude en roaming es el uso de un servicio móvil de un operador, mientras el usuario está fuera del país de "origen", sin la intención de pagar por las llamadas realizadas. El fraude en roaming es normalmente un fraude secundario, siendo el fraude de suscripción, el fraude primario, es decir, el defraudador tiene que obtener primero una suscripción a una red, utilizando

identidades falsas o robadas. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

El problema principal es el retardo en la transferencia de los registros de llamadas, entre las partes involucradas en el servicio roaming, este retardo puede significar hasta 72 horas antes que la red de origen reciba la información (en casos extremos, esto puede llegar a ser semanas). Este retardo en el monitoreo crea una ventana de oportunidad para el defraudador, y en ataques organizados, las pérdidas pueden ser extremadamente significativas, (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

Estimaciones de algunos sectores del mercado mundial indican que actualmente el fraude de roaming representa alrededor del 50% del fraude en GSM. Los operadores no solamente obtienen pérdidas por los ingresos no recaudados de las cuentas utilizadas para acceder el servicio, sino que también sufren pérdidas por el dinero que están obligados a pagar a sus socios de Roaming. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

Las pérdidas continúan incrementándose a medida que se van creando nuevas empresas y no hay avances reales o que se logren acuerdos en términos de transferir registros de las llamadas en tiempo real. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

El fraude se da cuando una vez en el extranjero, el usuario utiliza el servicio para llamar a otros destinos internacionales o a servicios de audiotexto ("premium rate services") con la intención de no pagar por ellos. Aunque en algunos casos involucran a individuos oportunistas, los casos más importantes son cometidos por organizaciones delictivas, quienes utilizan múltiples suscripciones fraudulentas para llevar acabo el ataque. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

El servicio de roaming es muy atractivo para el defraudador: el servicio es relativamente simple de obtener (a menudo es un servicio estándar, incluido con la conexión); ofrece un potencial de altas ganancias y los retardos en la transferencia de la información entre los entes involucrados en el servicio de

roaming, ayuda al defraudador a escapar de la detección. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

3.4.5. Robo de líneas telefónicas

Este tipo de fraude puede ser interno o externo, se da cuando líneas activas con asignación a usuarios son cambiadas de domicilio sin autorización del suscriptor o de la empresa local proveedora del servicio. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

Es uno de los fraudes más comunes por la facilidad de cometerlo en cualquier punto de la red externa. Generalmente esto es realizado por personal de mantenimiento, instaladores de planta externa o por ex-funcionarios de la compañía que conocen la distribución de la red. Las líneas telefónicas son utilizadas por terceros y el consumo es cobrado al suscriptor del servicio. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

La acometida de la red externa al domicilio del suscriptor es más vulnerable cuando es aérea, puede ser robada desconectando el cable del domicilio y llevándolo a otro lugar, también puede realizarse en un armario al desconectar el par del abonado y empatarlo con otro que va hacia otro lugar, o entrar a una caja y romper la protección del cable troncal, derivar un cable y conectarlo a otro del mismo cable troncal que va hacia el domicilio del defraudador. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

En sitios cerrados como edificios, se ingresan cables multipares que 1 convergen en una caja ubicada en el sótano "strip telefónico", desde este punto se reparten las líneas de abonado mediante multipares, el infractor conecta o deriva un par telefónico en cualquiera de los puntos y/o regletas instaladas en cada uno de los pisos del edificio y usualmente cambia constantemente el abonado que está derivando. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

La compañía prestadora del servicio se ve afectada ya que se produce un daño en la infraestructura y existe un aumento de reclamos por parte de los

clientes. De igual forma este tipo de fraude impacta directamente a la buena imagen de la compañía ante los clientes.

El usuario se ve afectado ya que cuando no se logra comprobar un fraude y/o uso indebido de la línea telefónica por parte de un tercero, debe pagar el monto total del consumo realizado por el defraudador. (Meza Ayala, Fraude en Roming, Robo de líneas Telefónicas, 2008)

3.4.6. By Pass

Etimológicamente, el término by pass es una palabra del idioma inglés, utilizada comúnmente para identificar a las derivaciones. Un sistema telefónico “by pass”, explicado de manera sencilla, consiste en registrar una llamada de origen internacional y, por tanto, que es facturada por la operadora telefónica como una llamada local. Desde el punto de vista tecnológico y práctico, esto es posible debido a que dicho sistema se implementa con tres elementos básicos e indispensables:

- Un enlace internacional para recibir el tráfico telefónico originado en el exterior; una instalación de equipos de telecomunicaciones, que efectúa el procesamiento de voz en cada llamada internacional recibida; y una considerable cantidad de líneas telefónicas utilizadas para terminar cada llamada internacional en la red de una operadora nacional. Todos estos elementos tecnológicos, una vez interconectados, configuran una verdadera ruta telefónica internacional, por supuesto, clandestina, paralela a las rutas legalmente establecidas por las operadoras autorizadas en el país. (Supertel, 2011)
- Un sistema by pass cursa llamadas telefónicas de origen internacional, hacia una red telefónica legalmente autorizada en el país. Por ende, su funcionamiento permite que se preste el Servicio Telefónico de Larga Distancia Internacional (STLDI) sin contar con el correspondiente título habilitante. (Supertel, 2011)

3.4.6.1. Ruta internacional autorizada

1. Desde el exterior, se puede realizar una llamada, que tiene por destino nuestro país, a través de un teléfono convencional o un celular de empresas telefónicas autorizadas en el exterior.

   Las llamadas pueden efectuarse por la operadora que brinda servicios de llamadas internacionales o mediante tarjetas prepago, que ofertan legalmente este mismo servicio.
2. La empresa telefónica en el exterior envía la llamada a nuestro país, la cual llega a la estación terrena de una operadora legalmente establecida, para que sea enrutada a través de la central de tránsito.
3. En la central de tránsito, por el código de acceso digitado, ésta es reconocida y facturada como llamada internacional, de acuerdo a las tasas internacionales de telefonía.
4. Una vez que es facturada llega a la central local, donde es enrutada a su destino final, es decir, el número que la persona en el exterior marcó. Esta llamada llega a la central local, previo acuerdo con la operadora en el exterior, ya que ambas han fijado una tarifa por esta conexión. De este acuerdo nace la legalidad del establecimiento de la llamada internacional.
5. Finalmente, la llamada llega al número de destino, el cual puede ser convencional o celular, de cualquier operadora legalmente establecida en nuestro país.

Figura 6. Ruta Legal de una llamada internacional.

Fuente: *(Supertel, 2011)*

3.4.6.2. Ruta internacional implementada con un sistema ilegal (By pass)

1. Se puede realizar una llamada desde el exterior hacia Ecuador, desde un teléfono fijo o celular. Ésta puede hacerse a través de tarjetas prepago no autorizadas, distribuidas y comercializadas por los defraudadores en locales informales, en el exterior, comercializadas a través de Internet. Debido al bajo precio de la tarjeta y a la gran cantidad de minutos que se compran y se venden, las personas las adquieren sin saber que la llamada va a ser cursada a través de una ruta ilegal.
2. Al marcar el número de destino en el exterior, la llamada es dirigida a través de una empresa telefónica hacia un carrier 1, que se encargará de enrutar la llamada hacia Ecuador.

   Empresas creadas exclusivamente para hacer by pass en nuestro país contactan a carriers en el exterior, y establecen un acuerdo comercial para que las llamadas sean enviadas a un telepuerto privado no autorizado. Es importante señalar que los carriers ignoran que estas empresas no poseen la correspondiente autorización en nuestro país para recibir y terminar llamadas internacionales.
3. Desde este telepuerto no autorizado, se envía la llamada hacia el lugar clandestino en el cual operan los defraudadores, en donde se hace el enrutamiento para terminarla en nuestro país.
4. Cuando la llamada llega desde el telepuerto no autorizado, los defraudadores se encargarán de cursarla hacia las diferentes redes telefónicas fijas o móviles nacionales.
5. Usando líneas fijas o celulares se cursa la llamada internacional como si fuera una local. La central local de una operadora telefónica autorizada, en nuestro país, las detecta como locales. De esta manera, se tarifa una llamada internacional como si fuera local, estableciéndose así el delito. (Supertel, 2011)

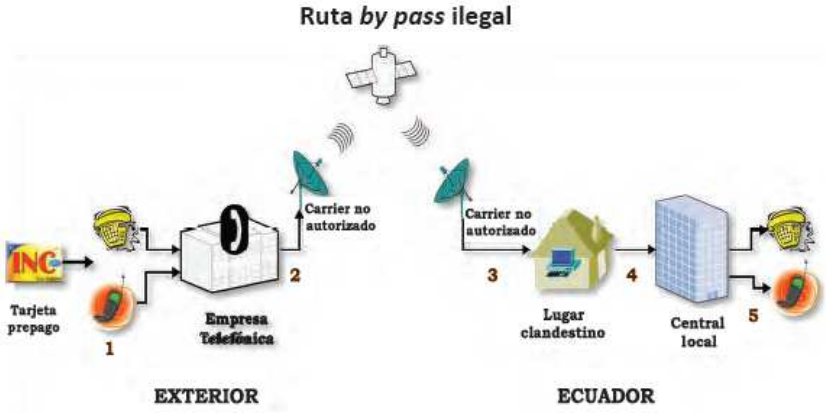

Figura 7. Ruta by pass ilegal.

Fuente: *(Supertel, 2011)*

3.4.6.3. Fraude de los sistemas by pass

El tráfico internacional que ingresa a nuestro país en relación al tráfico internacional saliente es de 5 a 1; es decir, por cada llamada internacional que se realiza se reciben cinco llamadas internacionales. Normalmente, éstas tienen un valor más alto que las locales.

Lo que permiten estos sistemas no autorizados es ocultar las llamadas internacionales y hacerlas pasar por locales. Por esta razón, implementar un sistema by pass en nuestro país es muy lucrativo para los defraudadores. Cabe mencionar que, al implementar una ruta by pass, no sólo la operadora de telefonía deja de percibir ingresos sino también el Estado ecuatoriano, ya que los impuestos que la operadora pagará serán mucho menores. Por lo tanto, los proyectos de telecomunicaciones planificados, sobre todo en áreas rurales, no podrían ser ejecutados. (Supertel, 2011)

3.5. Investigación tecnológica de los delitos de telecomunicaciones

Para los diversos casos de delitos en telecomunicaciones se van desarrollando varias técnicas para poder dar detectados.

3.5.1. Clonación de teléfonos celulares

- En caso de que su celular haya sido robado o se haya extraviado, debe informar a la operadora que le brinda el servicio de telefonía móvil y bloquear la línea.

- Se debe tratar de reparar el teléfono celular en locales autorizados por la operadora.
- Se están desarrollando técnicas basadas en triangulación pasiva, utilizando la red existente para detectar la ubicación del teléfono que se clono.
- Es importante revisar mensualmente la factura, para verificar posibles llamadas no efectuadas.
- En el caso de que se adquiera un aparato celular usado, se debe consultar a la operadora si éste no es robado. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

3.5.2. Call Back

No existe un método específico para la detección de este tipo de fraude, pero pueden considerarse ciertos aspectos que podrían ayudar a la detección:

La operadora telefónica puede realizar un análisis del comportamiento de las líneas que pertenecen a su red. Este tipo de fraude se detecta cuando se realiza gran cantidad de llamadas hacia un solo destino en el extranjero, con duración mínima. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Call back puede incluso escapar a las técnicas de detección, al ser implementado íntegramente con tecnología VolP (Meza Ayala, Fraudes en Telecomunicaciones, 2008). Aplicando esta tecnología la operadora solo cobrará como si se realizara una llamada local en vez de cobrar por una llamada internacional que se efectuó.

Con estas consideraciones, la detección de este tipo de fraude combinado, se hace posible realizar en dos etapas; la primera, con la identificación de los portales Web donde se ofrece el servicio "Call back" hacia nuestro país; la segunda, dotando de un identificador de llamadas, al terminal telefónico que recibirá la llamada internacional de retorno. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Entonces al hacer uso del servicio, será posible identificar los números de las líneas telefónicas utilizadas para terminar las llamadas internacionales de retorno en nuestro país.

Con los números telefónicos identificados, será posible efectuar las acciones técnicas necesarias para localizar el sitio donde se encuentra la infraestructura de telecomunicaciones utilizada para prestar este servicio ilegal. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

3.5.3. Fraude Tercer País

Este tipo de fraude se detecta por la irregularidad del consumo hacia destinos no comunes por parte de empresas suscriptoras del servicio, incremento en el consumo de llamadas internacionales o llamadas a países con historia de este fraude (países del medio oriente).

En el momento de ser detectada esta anomalía por parte del sistema de gestión, se debe verificar en el sistema de facturación el perfil del cliente, si es posible contactarlo y posteriormente realizar un corte del servicio de llamadas internacionales o nacionales salientes (esto depende de la regulación de cada uno de los países). (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

3.5.4. Fraude en Roaming

Cuando un suscriptor utiliza su teléfono en la red de otro operador, tiene lugar un proceso de autenticación, vía señalización SS73, entre la red visitada y la red de origen. De este requerimiento de autenticación, se puede extraer el país y la red que el suscriptor está visitando. Esta información es invaluable en la identificación del suscriptor que está haciendo roaming sin haber generado llamada alguna en la red de origen, lo cual es un fuerte indicador de fraude.

Se puede además realizar triangulaciones de autenticaciones y actualizaciones de ubicación, si un suscriptor continua realizando llamadas. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

3.5.5. Robo de Líneas Telefónicas.

El usuario realiza un reclamo por daño en la línea, y al verificarlo desde la central telefónica el abonado aparece activo; al realizar la revisión de la red

externa se encuentra la derivación o el traslado no autorizado. De igual forma, cuando un usuario que sea víctima de un robo reiterado y notorio (llamadas a larga distancia internacional, larga duración, alto coste, etc.), lo reporte al servicio de reclamos de la compañía. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Se debe realizar una demanda penal contra la persona que realizó la derivación. Si la derivación ocurrió en la acometida interna, deberá hacerlo el usuario ya que el debe responder por las llamadas realizadas a la Compañía, si es en cualquier otro punto de la red, el usuario no debe pagar los consumos realizados de manera fraudulenta y será la Compañía la que deberá actuar contra el defraudador. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Es importante ver específicamente el tráfico de llamadas en un horario en el que no se está en casa, debido a que esta franja es la usada por el defraudador para apropiarse ilícitamente de la línea. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

3.5.6. By Pass.

Para la detección se deberá adquirir tarjetas de telefonía internacional, con las que procede a realizar pruebas para detectar posibles Sistemas tipo "By pass", mediante un procedimiento llamado "Pruebas de Lazo o Loop", el procedimiento se detalla a continuación:

Se realiza una llamada mediante el uso de la tarjeta de telefonía internacional y se realiza la llamada desde el mismo país donde se quiere identificar el posible fraude.

Se siguen las instrucciones que aparecen en la parte posterior de la tarjeta y de este modo la llamada ingresa a la empresa telefónica en el "País B", se proporcionan los datos correspondientes al número de destino. Una vez que la llamada llevó a cabo su proceso, el terminal fijo o móvil usado recibirá una llamada; en caso de que dicha llamada sea enrutada legalmente, el número que aparecerá en el identificador será el correspondiente a un CARRIER legalmente establecido, caso contrario ("By pass"), el número que se visualizará, será un número local correspondiente a la operadora que está

siendo afectada por el fraude. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Una vez identificado el número o números que presuntamente pertenecerían a una instalación "By pass" se procede a realizar la investigación respectiva para saber a quién pertenecen dichos números. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

En el caso de que el número identificado corresponda a la serie de una Operadora de Telefonía Fija, la identificación del concesionario del número es relativamente fácil, ya que al ser "fijo", se conoce exactamente la ubicación física de la línea. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Sucede lo contrario en el caso de que el número detectado corresponda a la serie de un Operador de Telefonía Móvil, ya que a pesar de que la empresa operadora tenga toda la información del usuario a quien pertenece el número, es muy difícil identificar el lugar en que se encuentra el terminal de dicho número. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Técnicas para la ubicación de un Sistema "By pass"

En telefonía fija:

- Verificación en las Bases de Datos de la Empresa Operadora, para obtener la ubicación de la o las líneas según el o los números detectados.
- Verificación de los datos técnicos de instalación de las líneas. Seguimiento físico de los pares telefónicos. Identificación de la posición de los pares en el distribuidor telefónico.

En telefonía celular:

- Verificación de los datos personales de los clientes. Estudio de los parámetros técnicos de los aparatos celulares. Investigación sobre las características del enlace internacional. Estudio sobre el comportamiento de las líneas implicadas. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Prevención

Se debe mantener e intensificar las pruebas técnicas de tráfico telefónico internacional realizadas por cada operadora, para lograr determinar los números telefónicos que se están utilizando para cursar tráfico telefónico ilegal. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Conviene solicitar a las empresas de telefonía móvil celular, el cambio de las series numéricas de las líneas telefónicas celulares detectadas; y, de aquellas series que no están protegidas contra la clonación. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

Debe existir un estudio frecuente del tráfico generado y recibido por las líneas que pertenecen a cada operadora, en caso de detectar un comportamiento inusual, deberá precederse a la suspensión de dichas líneas, para evitar que se siga cursando tráfico ilegal.

Control

Adquisición de equipos dotados de hardware y software que, con algoritmos característicos del fraude, están en la capacidad de identificar la operación de sistemas fraudulentos.

Conformación de grupos de monitoreo permanentes, encargados de identificar el posible cometimiento de fraude telefónico.

Disposición de un grupo de élite, encargado de intervenir, desmontar y desarticular las bandas que clandestinamente prestan servicios ilegales de telecomunicaciones. (Meza Ayala, Fraudes en Telecomunicaciones, 2008)

CAPÍTULO IV

4. ANÁLISIS JURÍDICO

4.1. Delitos Informáticos en las normativas jurídicas ecuatorianas.

Los artículos son tomados de varios capítulos del Código Orgánico Integral Penal (COIP) publicado en el Registro Oficial el 10 de febrero de 2014; que contiene las infracciones y sanciones de delitos informáticos que se pueden llegar a ejecutar en Ecuador.

Los capítulos que hacen referencia a delitos informático son:

- En el Capítulo Segundo trata sobre delitos contra los derechos de libertad, en su SECCIÓN SEXTA menciona Delitos contra el derecho a la intimidad personal y familiar, citando los artículos:
    - Art. 178.- Violación a la intimidad
    - Art. 179.- Revelación de secreto.

  Dentro de este mismo capítulo en su SECCIÓN NOVENA menciona, Delitos contra el derecho a la propiedad, citando los artículos:
    - Art. 186.- Estafa
    - Art. 190.- Apropiación fraudulenta por medios electrónicos
    - Art. 191.- Reprogramación o modificación de información de equipos terminales móviles
    - Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles
    - Art. 193.- Reemplazo de identificación de terminales móviles
    - Art. 194.- Comercialización ilícita de terminales móviles
    - Art. 195.- Infraestructura ilícita

  También en este mismo capítulo en su SECCIÓN DECIMA menciona, Delitos contra el derecho a la identidad, citando el artículo:
    - Art. 212.- Suplantación de identidad

- En el Capítulo Tercero trata sobre delitos contra los derechos del buen vivir, en su SECCION TERCERA menciona Delitos contra la seguridad de los activos de los sistemas de información y comunicación, citando los artículos:
    - Art. 229.- Revelación ilegal de base de datos
    - Art. 230.- Interceptación ilegal de datos
    - Art. 231.- Transferencia electrónica de activo patrimonial.
    - Art. 232.- Ataque a la integridad de sistemas informáticos.
    - Art. 233.- Delitos contra la información pública reservada legalmente
    - Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

- En el Capítulo Sexto trata sobre delitos contra la estructura del estado constitucional, en su SECCION ÚNICA menciona Delitos contra la seguridad pública, citando el artículo:
    - Art. 354.- Espionaje

- En el Capítulo Séptimo trata sobre Terrorismo y su financiación, en su SECCION ÚNICA menciona Delitos contra la seguridad pública, citando el artículo:
    - Art. 366.- Terrorismo

Cuadro 1
Infracciones Informáticas

ARTICULOS	SANCION PRIVATIVA DE LIBERTAD	SANCIÓN MONETARIA
Artículo 178.- Violación a la intimidad.	Uno a tres años.	
Artículo 179.- Revelación de secreto.	Seis meses a un año.	
Artículo 186.- Estafa	Cinco a siete años.	Igual o mayor a cincuenta salarios básicos unificados del trabajador
Artículo 190.- Apropiación fraudulenta por medios electrónicos	Uno a tres años.	
Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles.	Uno a tres años.	
Artículo 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.-	Uno a tres años.	
Artículo 193.- Reemplazo de identificación de terminales móviles.	Uno a tres años.	
Artículo 194.- Comercialización ilícita de terminales móviles.	Uno a tres años.	
Artículo 195.- Infraestructura ilícita.	Uno a tres años.	
Artículo 212.- Suplantación de identidad	Uno a tres años.	
Artículo 229.- Revelación ilegal de base de datos	Uno a tres años.	
Artículo 230.- Interceptación ilegal de datos	Tres a cinco años.	
Artículo 231.- Transferencia electrónica de activo patrimonial.	Tres a cinco años.	
Artículo 232.- Ataque a la integridad de sistemas informáticos. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana	Tres a cinco años. Cinco a siete años	
Artículo 233.- Delitos contra la información pública reservada legalmente. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información	Cinco a siete años Tres a cinco años.	
Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	Tres a cinco años.	
Artículo 354.- Espionaje.	Siete a diez años	
Artículo 366.- Terrorismo	Diez a trece años	

4.2. Los delitos de telecomunicaciones en las normativas jurídicas ecuatorianas.

Los artículos son tomados del TÍTULO XIII de la LEY ORGÁNICA DE TELECOMUNICACIONES publicado en el Registro Oficial el 18 de febrero de 2015; que contiene el régimen sancionatorio de delitos en telecomunicaciones que se pueden llegar a ejecutar en Ecuador.

Los capítulos que hacen referencia a delitos en telecomunicaciones son:

- En el Capítulo Primero trata sobre infracciones, citando los artículos:
    - Art. 116.- Ámbito subjetivo y definición de la responsabilidad.
    - Art. 117.- Infracciones de primera clase.
    - Art. 118.- Infracciones de segunda clase.
    - Art. 119.- Infracciones de tercera clase.
    - Art. 120.- Infracciones cuarta clase.

- En el Capítulo Segundo trata sobre sanciones, citando los artículos:
    - Art. 121.- Clases.
    - Art. 122.- Monto de referencia.
    - Art. 123.- Destino de las multas.

Cuadro 2
Infracciones Telecomunicaciones.

ARTICULOS	MULTA	MONTO DE REFERENCIA
Artículo 117.- Infracciones de primera clase.	0,001% y el 0,03% del monto de referencia.	Cien Salarios Básicos Unificados del trabajador en general.
Artículo 118.- Infracciones de segunda clase.	0,031% al 0,07% del monto de referencia.	Ciento uno hasta trescientos Salarios Básicos Unificados del trabajador en general.
Artículo 119.- Infracciones de tercera clase.	0,071% y el 0,1 % del monto de referencia.	Trescientos uno hasta mil quinientos Salarios Básicos Unificados del trabajador en general.
Artículo 120.- Infracciones cuarta clase.	1% del monto de referencia.	Mil quinientos uno hasta dos mil Salarios Básicos Unificados del trabajador en general.

4.3. Análisis de las normativas jurídicas ecuatorianas con los delitos informáticos y de telecomunicaciones.

Los tipos de delitos informáticos y de telecomunicaciones que se han investigado en los puntos 4.1 y 4.2, si se encuentran contemplados en varios artículos de las leyes ecuatorianas.

Datos falsos o engañosos (Data diddling), se la puede contemplar dentro COIP en los artículos:

- Art. 178.- Violación a la intimidad.
- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 230.- Interceptación ilegal de datos. Inciso Número 1.
- Art. 232.- Ataque a la integridad de sistemas informáticos.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Manipulación de programas o los “caballos de troya” (Troya Horses), se la puede contemplar dentro COIP en el artículo:

- Art. 232.- Ataque a la integridad de sistemas informáticos. Incisos Números 1 y 2.

Se puede citar este artículo ya que en su texto original cumple con todas las características de este delito que se señalan como el de alterar, modificar, borrar y otras modificaciones que se realicen a programas, sistemas de tratamiento de información, telemático o de telecomunicaciones.

Se sancionara con pena privativa de libertad de tres a cinco años.

La técnica del salami (Salami Technique/Rounching Down), se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos
- Art. 231.- Transferencia electrónica de activo patrimonial

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el que utilice 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; alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones que trata de cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Falsificaciones informáticas, se la puede contemplar dentro COIP en los artículos:

- Art. 178.- Violación a la intimidad
- Art. 186.- Estafa. Inciso número 1.
- Art. 231.- Transferencia electrónica de activo patrimonial.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de cinco a siete años.

Manipulación de los datos de salida, se la puede contemplar dentro COIP en los artículos:

- Art. 186.- Estafa. Incisos números 1 y 2.
- Art. 190.- Apropiación fraudulenta por medios electrónicos
- Art. 230.- Interceptación ilegal de datos. Inciso número 3.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como alterar, clonar, duplicar, copiar, robar la información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en tarjetas de crédito, débito, pago o similares sin el consentimiento de su propietario, esto se lo realiza mediante el uso de dispositivos electrónicos, que también se los utiliza en cajeros automáticos.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de cinco a siete años.

Pishing, se la puede contemplar dentro COIP en los artículos:

- Art. 178.- Violación a la intimidad.
- Art. 186.- Estafa. Inciso número 1.
- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 212.- Suplantación de identidad
- Art. 230.- Interceptación ilegal de datos. Inciso número 2.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, también clonar, duplicar, copiar, robar la información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en tarjetas de crédito, débito, pago o similares. Se lo realiza por medio de un sistema informático que ejecute, programe y envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o que modifique el sistema de resolución de nombres de dominio de un servicio

financiero de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de cinco a siete años.

Bombas lógicas (logic bombs), se la puede contemplar dentro COIP en el artículo:

- Art. 232.- Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2.

Se puede citar este artículo ya que en su texto original cumple con todas las características de este delito que son que una persona diseñe, desarrolle, programe, destruya, altere, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos para causar mal funcionamiento en los sistemas de tratamientos de información, como también en la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Se sancionara con pena privativa de libertad de tres a cinco años.

Gusanos, se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 232.- Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, como también en la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Virus informáticos y Malware, se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 232.- Ataque a la integridad de sistemas informáticos. Inciso números 1 y 2.
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, como también en la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Ciberterrorismo, se la puede contemplar dentro COIP en el artículo:

- Art. 366.- Terrorismo. Número 1.

Se puede citar este artículo ya que en su texto original cumple con todas las características de este delito como, si una persona individualmente o formando asociaciones armadas, haga uso de medios tecnológicos para amenazar, intimidar, destruir, causar daños o pongan en peligro a la población.

Se sancionara con pena privativa de libertad de diez a trece años.

Ataques de denegación de servicio, se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 232.- Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, como también en la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Fuga de datos (Data Leakage), se la puede contemplar dentro COIP en los artículos:

- Art. 178.- Violación a la intimidad.
- Art. 229.- Revelación ilegal de base de datos.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático en este caso la revelación de base de datos, por medio de un sistema informático, electrónico o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son

subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de uno a tres años.

Hurto del tiempo del computador, se la puede contemplar dentro COIP en los artículos:

- Art. 229.- Revelación ilegal de base de datos.
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático en este caso la revelación de claves para uso de internet, por medio de un sistema informático, electrónico o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Parasitismo informático (piggybacking) y suplantación de personalidad (impersonation), se las pueden contemplar dentro COIP en los artículos:

- Art. 178.- Violación a la intimidad.
- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 212.- Suplantación de identidad

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de obtener, acceder, interceptar, retener, grabar, reproducir en cualquier forma un dato informático o suplantar la identidad de una persona para cometer actos ilícitos, por medio de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años.

Puertas falsas (trap doors), se la puede contemplar dentro COIP en los artículos:

- Art. 230.- Interceptación ilegal de datos. Número 1.
- Art. 232.- Ataque a la integridad de sistemas informáticos. Inciso número 1 y 2.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de acceder, interceptar, retener, grabar, introducir, destruir o alterar en cualquier forma un dato informático, a través de un sistema informático o redes electrónicas y de telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de cinco a siete años.

Llave maestra (superzapping), se la puede contemplar dentro COIP en los artículos:

- Art. 230.- Interceptación ilegal de datos. Inciso número 1.
- Art. 232.- Ataque a la integridad de sistemas informáticos. Número 1 y 2.
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el de acceder, interceptar, retener, grabar, introducir, destruir, alterar o utilizar en cualquier forma un dato informático, a través de un sistema informático o redes electrónicas y de

telecomunicaciones, sin contar con el consentimiento o la autorización legal de una persona o de sistemas de tratamiento de información, telemático o de telecomunicaciones.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de cinco a siete años.

Clonación de teléfonos celulares, se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.-
- Art. 191.- Reprogramación o modificación de información de equipos terminales móviles
- Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.
- Art. 193.- Reemplazo de identificación de terminales móviles
- Art. 194.- Comercialización ilícita de terminales móviles.
- Art. 195.- Infraestructura ilícita.
- Art. 212.- Suplantación de identidad
- Art. 232.- Ataque a la integridad de sistemas informáticos. Inciso número 1
- Art. 234.- Acceso no consentido a un sistema informático.

Dentro de este mismo delito se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en el artículo:

- Art. 118.- Infracciones de segunda clase. Literal a, número 2.
- Art. 119.- Infracciones de tercera clase. Literal a, número 1.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como que, una persona utilice, altere, manipule, modifique, reprograme, comercialice, cause interferencias fraudulentamente a sistemas informáticos, redes electrónicas y de telecomunicaciones o terminales móviles; para facilitar la apropiación de sistemas de tratamiento de información, telemático o de telecomunicaciones,

así también para la prestación de servicios no autorizados regulados por el Ministerio de las Telecomunicaciones y de la Sociedad de la Información o la Agencia de Regulación y Control de las Telecomunicaciones .

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 1% del monto de referencia que va de Mil quinientos uno hasta dos mil Salarios Básicos Unificados del trabajador en general.

Call back o llamada revertida, se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en los artículos:

- Art. 117.- Infracciones de primera clase. Literal a, número 1.
- Art. 118.- Infracciones de segunda clase. Literal a, número 2.
- Art. 119.- Infracciones de tercera clase. Literal a, número 1.

Dentro de este mismo delito se la puede contemplar dentro COIP en el artículo:

- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el acceso no consentido a un sistema informático, telemático o de telecomunicaciones sin la autorización de sus propietarios, una vez logrado el ingreso al sistema se podrá: utilizar, desviar, modificar, redireccionar, causar interferencias en el tráfico de datos o voz y con esto se logra proveer u ofrecer servicios que estos sistemas proveen a terceros, sin pagar a los proveedores de servicios legítimos.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 0,071% y el 0,1 % del monto de referencia que va

de Trescientos uno hasta mil quinientos Salarios Básicos Unificados del trabajador en general.

Fraude tercer país, se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en los artículos:

- Art. 117.- Infracciones de primera clase. Literal a, número 1.
- Art. 118.- Infracciones de segunda clase. Literal a, número 2.
- Art. 119.- Infracciones de tercera clase. Literal a, número 1.

Dentro de este mismo delito se la puede contemplar dentro COIP en el artículo:

- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el acceso no consentido a un sistema informático, telemático o de telecomunicaciones sin la autorización de sus propietarios, una vez logrado el ingreso al sistema se podrá: utilizar, desviar, modificar, redireccionar, causar interferencias perjudiciales en el tráfico de datos y voz; con esto se logra proveer u ofrecer servicios sin pagar a los proveedores legítimos.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 0,031% y el 0,7 % del monto de referencia que va de Ciento uno hasta trescientos Salarios Básicos Unificados del trabajador en general.

Fraude en roaming, se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en los artículos:

- Art. 117.- Infracciones de primera clase. Literal a, número 1.
- Art. 118.- Infracciones de segunda clase. Literal a, número 2.

Dentro de este mismo delito se la puede contemplar dentro COIP en los artículos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 212.- Suplantación de identidad.
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el acceso no autorizado mediante la suplantación de identidad para obtener un beneficio en este casa será el de modificar, desviar o redireccionar tráfico de voz y de datos sin que los proveedores de este servicio cobren por estos causando así interferencias perjudiciales en el servicio que ofrecen. Esto se lo puede hacer mediante el uso de equipos terminales que no son homologados o no cumplan las condiciones técnicas autorizadas.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 0,031% y el 0,7 % del monto de referencia que va de Ciento uno hasta trescientos Salarios Básicos Unificados del trabajador en general.

Robo de líneas telefónicas, se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en los artículos:

- Art. 118.- Infracciones de segunda clase. Literal a, número 2.
- Art. 119.- Infracciones de tercera clase. Literal a, número 1.

Dentro de este mismo delito se la puede contemplar dentro COIP en los artículos:

- Art. 186.- Estafa. Número 3.
- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 212.- Suplantación de identidad.
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el acceso no autorizado mediante la suplantación de identidad para obtener un beneficio en este casa será el de modificar, desviar o redireccionar tráfico de voz y de datos sin que los proveedores de este servicio cobren por estos causando así interferencias perjudiciales en el servicio que ofrecen. Esto se lo puede hacer mediante el uso de equipos terminales que no son homologados o no cumplan las condiciones técnicas autorizadas.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 0,031% y el 0,7 % del monto de referencia que va de Ciento uno hasta trescientos Salarios Básicos Unificados del trabajador en general.

By pass, se puede contemplar dentro de la LEY ORGÁNICA DE TELECOMUNICACIONES en los artículos:

- Art. 118.- Infracciones de segunda clase. Literal a, número 2.
- Art. 119.- Infracciones de tercera clase. Literal a, número 1.

  Dentro de este mismo delito se la puede contemplar dentro COIP en el artículo:
- Art. 234.- Acceso no consentido a un sistema informático.

Se puede citar estos artículos ya que en su texto original cumple con todas las características de este delito como el acceso no consentido a un sistema informático, telemático o de telecomunicaciones sin la autorización de sus propietarios, una vez logrado el ingreso al sistema se podrá: utilizar, desviar, modificar, redireccionar, causar interferencias perjudiciales en el tráfico de datos y voz; con esto se logra proveer u ofrecer servicios sin pagar a los proveedores legítimos.

Para la sanción se aplicara el Artículo 21 del COIP; que trata sobre el Concurso ideal de infracciones.- Cuando varios tipos penales son subsumibles a la misma conducta, se aplicará la pena de la infracción más grave. La cual es la privativa de libertad de tres a cinco años. También habrá una sanción económica del 0,031% y el 0,7 % del monto de referencia que va de Ciento uno hasta trescientos Salarios Básicos Unificados del trabajador en general.

4.4. Casos de delitos informáticos sancionados en Ecuador con el Código Orgánico Integral Penal (COIP).

Según datos recopilados por la Fiscalía del Ecuador y expuestos en un boletín publicado el 13 de junio del 2015, los delitos más comunes son: Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, acoso sexual.

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 cuando entró en vigencia el Código Orgánico Integral Penal (COIP) hasta el 31 de mayo del 2015. (Fiscalia General del Estado del Ecuador, 2015)

Según el fiscal Edwin Pérez, especialista en delitos informáticos, indicó que en Ecuador existen dificultades durante la investigación, por la información cruzada a nivel de redes sociales o cuentas de correos electrónicos, ya que los grandes proveedores de las redes sociales y generadores de los sistemas informáticos como Google, Facebook, Yahoo, entre otros, tienen los bancos de datos de sus usuarios en Estados Unidos y solicitar esa información puede demorar meses. Además el país no cuenta con convenios internacionales que faciliten el cruce de datos informáticos como los que existe entre Estados Unidos y Europa. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información. (Fiscalia General del Estado del Ecuador, 2015)

En la figura 9 tomada del boletín de la fiscalía se puede observar cómo ha ido creciendo y a la ves disminuyendo los delitos informáticos desde el 2009 hasta mayo del 2015. Y en que ciudades se comenten más ilícitos.

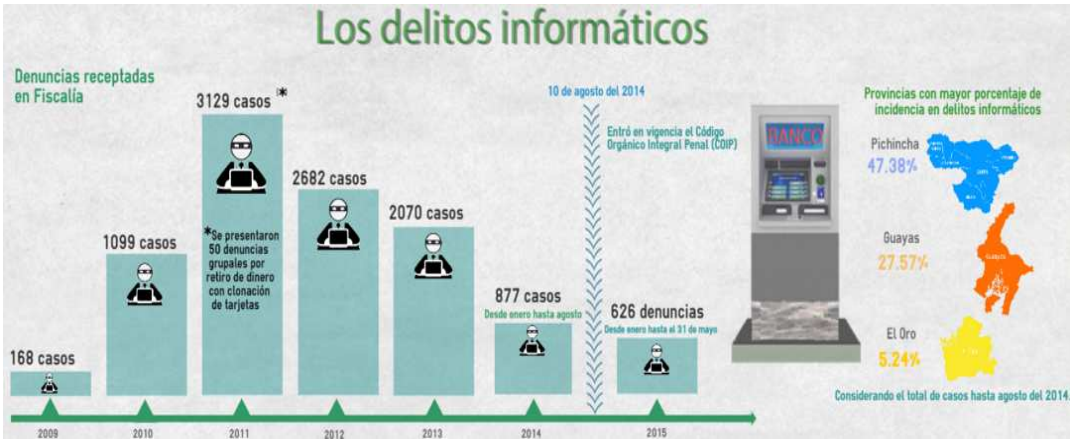

Figura 8. Delitos informáticos.
Fuente: *(Fiscalia General del Estado del Ecuador, 2015)*

En mayo del 2014, una persona denunció que había sido víctima del delito de apropiación ilegal de datos, la victima solo recuerda que ingresó sus datos para realizar una compra por Internet, porque se ofrecían descuentos en productos de belleza. El delincuente utilizo los datos y su tarjeta de crédito para realizar algunas compras, el monto total fue de 2.500 dólares. En estos momentos la fiscalía se encuentra investigando su caso. Con el COIP la sanción que podría recibir la persona que robó sus datos, podría ser una pena de uno a tres años de cárcel. (Fiscalia General del Estado del Ecuador, 2015)

Otra delito informático denunciado fue la interceptación ilegal de datos esta vez la víctima fue Mauricio E., de 21 años. Con los datos obtenidos bloquearon su cuenta en Facebook y luego alguien publico comentarios ofensivos y subía fotos en su nombre. Este joven tuvo que enviar mensajes de texto, llamar por teléfono y redactar correos a sus contactos explicando que no era el autor de insultos a otras personas en la red. El delito de interceptación ilegal de datos consta en el artículo 230 del COIP. Este sanciona con tres a cinco años de pena privativa de libertad a quienes utilicen estos datos y los difundan. (Fiscalia General del Estado del Ecuador, 2015)

El mismo presidente Rafael Correa también denunció que su cuenta de Twitter fue hackeada en marzo del 2014. Horas después adjudicó los ataques a “la extrema derecha de ciertos países extranjeros, en complicidad con inescrupulosos opositores nacionales”. Un día después dos jóvenes fueron detenidos y más tarde liberados. El artículo 178 del COIP señala que la persona que, sin consentimiento, acceda, difunda o publique datos íntimos de un correo electrónico, de una computadora, plataforma de chats o cualquier red social será sancionada con uno y hasta tres años de cárcel. (Diario EL COMERCIO, 2015)

También está el robo de datos es cuando una persona duplica una página institucional como la de un banco o de una compañía de comercio electrónico y, sin advertir que es falsa, el usuario realiza alguna transacción. Un mecanismo para captar a un victima son los mensajes mediante correo electrónico. En estos se pide, por ejemplo, actualizar la información de la tarjeta de crédito, con la supuesta advertencia de que si no se cumple en 24 horas se cancelará la misma. (Fiscalia General del Estado del Ecuador, 2015)

Eso ocurrió con Lorena A., de 31 años. Este delito se lo realizo en febrero del 2015 tras recibir un correo, ella sin percatarse actualizó su información. Pero luego se dio cuenta de que alguien había consumido 1.200 dólares de su tarjeta de crédito. La afectada denunció el hecho en la Fiscalía y ahora su caso se investiga, ya que se debe solicitar informes a los bancos sobre las transacciones para tratar de descubrir al responsable. Por ser un delito informático, el tiempo del proceso se alarga hasta dar con el timador. (Fiscalia General del Estado del Ecuador, 2015)

CAPÍTULO V

5. PROPUESTAS NACIONALES A LA SEGURIDAD DE LA INFORMACIÓN.

5.1. Esquema Gubernamental de Seguridad de la Información EGSI.

El Esquema Gubernamental de Seguridad de la Información (EGSI), se basa en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información. Que establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública.

Estas directrices la deben aplicar:

- La Administración Pública de forma integral y coordinada debe minimizar o anular riesgos en la información; así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos.
- Las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional, que deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

En los capítulos número: uno, tres, cinco, seis, siete del EGSI que hace mención a diferentes métodos para dar seguridad y mantener ordenada la información. Dentro de los más importantes son:

- Política de Seguridad: Hace mención a que se debe tener documentación y políticas para garantizar la seguridad de la información. Esto se puede realizar definiendo de manera formal una política de seguridad que manifieste los objetivos, alcance e importancia de la seguridad de la información en las instituciones que se acojan al EGSI.
- Gestión de Activos: En las instituciones que acojan el EGSI es de suma importancia que se ponga en práctica todas las normas que se

mencionan en este capítulo, en el contenido esta realizar un inventario de activos en formatos físicos (hardware) y electrónicos (software), ya que con esto se podrá conocer todas las características y ver el estado en el que se encuentran los activos.

El inventario también se debe considerar activos referentes a la estructura organizacional que incluyan todas las unidades administrativas con los cargos y nombres de las autoridades, así también estructura organizacional del área de las TIC con toda la información referente a sus cargos.

Una parte importe de este capítulo está en el punto 3.3 que es “Uso aceptable de los activos”, que hace referencia al monitoreo de la red interna con lo que se podrá reglamentar el acceso y uso de la Internet, lo que con lleva varias reglas como que cada usuario es responsable de la información y contenidos a los que accede, así como también bloquear y prohibir el acceso a redes sociales, otra es la de prohibir el uso de servicios de correo electrónico en la Internet.

Además se podrá en un futuro establecer mecanismos de control para verificar la existencia de un activo realizando una comparativa con una base de datos que se generara una vez finaliza el inventario.

- Seguridad Física y del Entorno: En este capítulo hace referencia a controles de acceso físico a las instalaciones y equipos de la institución que apliquen el EGSI, es necesario realizar un seguimiento del personal y visitantes que acceden a las áreas críticas de la institución, para el control de esto se debe iimplementar el uso de una identificación visible para todo el personal y visitantes, así como también si van a áreas restringidas deberán ser escoltados por una persona autorizada. Además los equipos de procesamiento de información deben estar en áreas completamente seguras para protegerlos de acceso no autorizado y amenazas externas o ambientales. También se deberá revisar la protección del cableado, aplicando todas las normas locales e internacionales para el manejo del sistema de cableado. Así como

realizar procedimientos para el mantenimiento de equipos, de tal forma que se mantenga la seguridad de la información.

- Gestión de Comunicaciones y Operaciones: Lo que en este capítulo recomienda es: separar los ambientes de desarrollo, prueba y operación; definir directrices para la protección contra código malicioso, gestionar los respaldos de información, definir políticas y procedimientos para el intercambio de información dentro de esto se encuentra dar control y seguridad de las redes de datos que se encuentren en la institución, así como también monitorear el uso del sistema por medio de software que nos den alertas o notificaciones si algún usuario está realizando actos que le competen. Todo lo mencionado anterior lo debe ejecutar y poner en conocimiento de todo el personal de la institución el área de Tecnologías de la Información (TIC).
- Control de Acceso: Este capítulo recomienda crear una política de control de acceso en la cual se asegure el ingreso de usuarios autorizados y previniendo los accesos no autorizados, también se debe gestionar privilegios de distintos niveles a ciertos usuarios basándose en las actividades y necesidades que cumpla dentro de la institución. También se debe tener control sobre las conexiones, enrutamiento de las redes realizando la configuración de los diferentes equipos que se ocupan en la red de la institución, así como también la protección de los puertos de red.

5.2. Comando de Ciberdefensa.

El termino Ciberdefensa es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

En Ecuador el comando de Ciberdefensa está contemplado en La Agenda Política de la Defensa (APD) 2014-2017 del Ministerio de Defensa Nacional. Debido que el país es uno de los 10 países que está en el blanco de ataques

cibernéticos. Frente a los ataques informáticos el Estado busca blindarse con la creación de un comando de operaciones.

Este comando inició su trabajo el 4 de noviembre del 2014 con un presupuesto inicial de 8 millones de dólares.

La misión del comando de Ciberdefensa es el defender, explotar y responder ante amenazas y factores de riesgo en el dominio del ciberespacio, que atenten a la seguridad de la infraestructura crítica estratégica del Estado; en forma permanente.

En el país funciona el Comando Uno Norte, que abarca Esmeraldas, Carchi, Imbabura, Sucumbíos, Orellana, Napo, Pastaza y Morona Santiago.

El Comando Dos, con área de influencia en Guayas, Manabí, Los Ríos, Santa Elena, Galápagos.

El Comando Tres en el sur, con Cañar, Azuay, Zamora Chinchipe, Loja, El Oro.

El Comando Cuatro Central para Pichincha, Cotopaxi, Tungurahua, Chimborazo, Bolívar, Santo Domingo de los Tsáchilas.

Y el Comando Cinco de Operaciones Aérea y Defensa que refuerzan los trabajos en Guayas, Manabí y Pichincha.

Dentro de las capacidades que tiene el comando de ciberdefensa están

- Evitar el acceso no autorizado por parte de agentes extraños a los sistemas de información; redes de telecomunicaciones estatales y a sistemas de control y operación de la infraestructura estratégica civil y militar
- Diagnosticar las capacidades cibernéticas de potenciales adversarios, de agentes hostiles y de las redes propias;
- Adoptar medidas de prevención y detección frente ataques, interrupciones, acciones hostiles, que puedan comprometer los sistemas de información.
- Ejecutar acciones de respuesta oportuna ante amenazas o ataques cibernéticos localizados.

Figura 9. Estructura organizacional por procesos comando de ciberdefensa en FF.AA.

Actualmente, esta unidad ejecuta acciones de respuesta inmediata ante ataques; inició procesos de capacitación de personal militar y civil para su incorporación institucional a tareas técnico-operativas; y se encuentra inventariando la infraestructura tecnológica existente en el Sector Defensa a la vez que implementa estrictas medidas de seguridad informática.

El fortalecimiento de la ciberdefensa también está encaminado a precautelar la privacidad y combatir los delitos transnacionales.

5.3. Propuesta de ley de protección de datos.

Los datos es toda información que se refiere a cualquier dato de una persona, puede ser identificado por medio de informaciones como: el nombre, la dirección, la de nacimiento, la nacionalidad, sexo, antepasados, estado civil, situación económica, situación financiera, profesión, religión, costumbres y familia, etc.

En el ámbito público, los Estados a través de los años han creado registros públicos, como, registro civil y así se han hecho presente otros, como el de registro de antecedentes penales y carcelarios en casi toda la región, últimamente en nuestro país se aprobó la Ley Orgánica de Registro de Datos

Públicos; muchas son las instituciones públicas que en su poder tienen información personal, archivos o bases de datos, como el Servicio de Rentas Internas, el Instituto de Seguridad Social, Dirección Nacional de Migración, Dirección Nacional de Tránsito, Dirección Nacional de Registro Civil, Identificación y Cedulación, Policía Nacional, Comisión de Tránsito del Guayas, Ministerio de Relaciones Laborales, Instituto Ecuatoriano de Propiedad Intelectual, Municipalidades, Función Judicial, Fiscalía General del Estado; los servicios públicos, escuelas, hospitales, telefonía, agua, electricidad, registran datos personales e información, que no son necesarios hacerlos públicos, sino mantenerlos en reserva y protegidos por tener el carácter de sensibles.

En lo privado, desde años atrás se da un proceso de recolección de datos personales, ejemplo, la Banca, empresas prestadoras de salud, de educación, de asuntos contables, y otros servicios, entre las diferentes instituciones se comparten datos que en algún momento vulneran los derechos y garantías constitucionales. Se han generado registros, archivos, o bancos de datos sin restricción alguna, se constata como bancos, empresas de toda naturaleza, tarjetas de crédito, compañías áreas, correlacionan y ceden datos personales, que a veces resultan de utilidad y en otros casos perjudicial debido a la inseguridad, dándose lugar a un comercio ilegal de datos como se ha anotado anteriormente, circunstancias que no puede darse en un Estado Constitucional de Derechos y Justicia, como se encuentra concebido nuestro país en la Constitución de la República.

Análisis de la Ley del Sistema Nacional del Registro de Datos Públicos

Como norma general se señala que los registros de datos públicos administrarán sus bases de datos en coordinación con la Dirección Nacional de Registro de Datos Públicos de acuerdo a un Reglamento que deberá dictarse con tal propósito.

EL Art. 30 de la Ley del Sistema Nacional de Registro de Datos Públicos expresa: “Créase la Dirección Nacional de Registro de Datos Públicos, como organismo de derecho público, con personería jurídica, autonomía

administrativa, técnica, operativa, financiera y presupuestaria, adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información. Su máxima autoridad y representante legal será la Directora o Director Nacional, designada o designado por la Ministra o Ministro. Su sede será la ciudad de Quito, tendrá jurisdicción nacional, y podrá establecer oficinas desconcentradas a nivel nacional."

Con el registro de datos públicos de personas naturales y jurídicas, se tendrá información privada de lo que tiene una persona, lo que con lleva, que la información sobre el patrimonio de las personas será de libre acceso, lo que coloca en total estado de indefensión a las personas, frente a los extorsionadores y delincuentes.

Sobre los datos personalísimos como etnia, estado de salud, orientación sexual, religión, condición migratoria y otras atientes a la intimidad personal, y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución y en los instrumentos internacionales o contra la seguridad interna y externa del Estado, son confidenciales y su acceso sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.

De lo anterior no debe constar en un registro de datos públicos, y las condiciones para su otorgamiento son una trampa, pues por mandato de la ley se puede violar la constitución, sobre todo en un país donde el poder total será centralizado y no hay organismos independientes a los que acudir. Los registros son dependencias públicas desconcentradas, con autonomía registral y administrativa en los términos de la ley y sujetos al control, auditoría y vigilancia, de la Dirección Nacional de Registros de Datos Públicos conforme se determine en el respectivo reglamento de la Ley.

En este contexto se evidencia un gran riesgo debido al acceso y conocimiento de datos personales y su uso para fines ilícitos por parte de terceras personas, por lo que ante este desafío de las nuevas tecnologías, es imprescindible, impostergable y urgente un marco legal adecuado que garantice un tratamiento seguro de la información personal que se encuentran

en manos de entidades públicas y privadas, una legislación que vaya a la vanguardia del desarrollo y avance de las tecnologías.

TRATADOS INTERNACIONALES SOBRE EL DERECHO CONSTITUCIONAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Se menciona los siguientes:

a) Convención Europea de Salvaguardia de los Derechos del Hombre y las Libertades Fundamentales, que en su Art. 18.1 dice, que toda persona tiene derecho a su vida privada.

b) La Convención Americana de Derechos Humanos de 1969, que se la conoce como Pacto de San José de Costa Rica, que en el Art. 25 se reconoce, que toda persona tiene derecho a un recurso sencillo y práctico, que lo ampare contra actos que violen los derechos fundamentales reconocidos por la Constitución y la ley; y, entre ellos el de la vida privada.

c) La Declaración Americana de Derechos y Deberes del Hombre, aprobada en la IX Conferencia Interamericana en la ciudad de Bogotá Colombia, en 1948.

d) La Declaración Universal de Derechos Humanos, aprobados por la Organización de las Naciones Unidas, que en su Art. 12 garantiza este derecho.

e) El Pacto Internacional de Derechos Civiles y Políticos, firmado en Nueva York el 19 de diciembre de 1966, que en su Art. 17 garantiza el derecho antes mencionado.

f) La Convención Europea de Salvaguardia de los Derechos del Hombre y Libertades Fundamentales; Art. 8.1. Convenio No. 108.

g) Tratado de la Unión Europea de 07 de febrero de 1992, en su Art. 72 trata sobre este derecho.

h) El Parlamento Europeo ha dictado varias Resoluciones en el año de 1989, especialmente en los Arts. 6 y 18.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES.

6.1. CONCLUSIONES.

- Los delitos informáticos y de telecomunicaciones en la actualidad tienden a aumentar debido a avances tecnológicos y esto lleva a que exista un gran interés por parte de los gobiernos e instituciones especializadas para poder contrarrestar e investigar este tipo de conductas. Ya que se podrán implementar políticas, planes para combatir los delitos que se comentan en Ecuador.
- En la actualidad existen diversas formas para realizar estos delitos mediante la ingeniería social, engaños o utilizando métodos avanzados para el ingreso en sistemas informáticos y de telecomunicaciones con el objetivo de copiar, borrar, modificar, transferir información y con esto lograr que en pocos segundos colapsen varios sistemas informáticos, como también afectar la privacidad de las personas ya que en algunas ocasiones estos datos obtenidos de manera ilegal se los pueden vender por grandes sumas de dinero.
- La mayoría de personas o empresas (sujetos pasivos), no denuncian estos delitos, con el objetivo de evitar el desprestigio por un fallo en la seguridad. Las víctimas prefieren asumir las consecuencias del delito e intentar prevenirlo para el futuro utilizando métodos más sofisticados para la protección de sus sistemas.
- A los delincuentes de delitos informáticos y de telecomunicaciones se los puede diferenciar de un delincuente común, ya que estos poseen habilidades para acceder y manipular sistemas informáticos con gran facilidad, existe una clase que no se la llamaría delincuente, sino que toma el nombre de hacker ético, este es el encargado de buscar todas las vulnerabilidades que puede tener una institución; este realizará un análisis minucioso y entregara un informe detallado de todos los problemas en seguridad informática encontrados en la institución que se realizó el análisis.

- La mayoría de los cyberdelincuentes son empleados internos y estos reconocen dónde se encuentra localizada la información de vital importancia para la institución. Lo hacen con el objetivo de tener alguna retribución económica por la venta de esta información.
- En el mundo de la informática y de las telecomunicaciones existen diversos tipos de delitos, en este trabajo se los ha clasificado de acuerdo a su intencionalidad como: fraude, sabotaje informático, robo de servicios, acceso no autorizado a servicios informático, espionaje informático y el robo o hurto de software; con esta división se ha conseguido realizar un análisis con los artículos de las leyes ecuatorianas (COIP y Ley de Orgánica de Telecomunicaciones) que están en vigencia ya que en sus textos se indica si se está cometiendo algún acto ilícito empleando medios tecnológicos, como también la sanción en el caso ser declarado culpable.
- Uno de los principales problemas que se considera en delitos informáticos y de telecomunicaciones, es la obtención de pruebas para que pueden ser juzgados los delincuentes que cometen actos ilícitos; ya que en muchos de los casos no se tiene el conocimiento y herramientas necesarias para poder obtener pistas y posteriormente llevarlo ante las autoridades competentes.
- A medida que la tecnología evoluciona se desarrolla hardware y software para la detección oportuna de los delitos y se logrará proveer una infraestructura robusta para que pueda soportar el cometimiento de actos ilícitos.
- En Ecuador se está comenzando a contrarrestar este tipo de delitos con la creación de leyes y organismos estatales encargados de proteger los sistemas informáticos y de telecomunicaciones con el fin de poder detectar, sancionar y notificar cuando se estén produciendo los actos ilícitos.

- En las universidades donde existe carreas de informática y telecomunicaciones, se debería implementar asignaturas dedicadas para dar a conocer a sus estudiantes, qué clase de delitos se pueden cometer y si los mismo tienen una sanción en las leyes del Ecuador, lo que llevaría a estar más capacitados en el tema y con la finalidad de desarrollar proyectos, software para la correcta mitigación de los delitos.

6.2. RECOMENDACIONES.

- Se debe estar actualizado en temas sobre delitos informáticos, para poder contrarrestar; en especial los funcionarios de TIC, de cada institución ya que son ellos los manejan todos los sistemas de seguridad de datos como también el acceso a internet ya que esta es la puerta de conexión con gran nube que existe en el mundo.
- Se debe tener cuidado y aplicar métodos de seguridad informática en sistemas domésticos o empresariales para contrarrestar y evitar al máximo sufrir las consecuencias de acciones ilegales.
- Se debe generar profesionales especializados en el estudio de delitos informáticos y de telecomunicaciones; para que puedan responder a la creciente necesidad de la sociedad de contar con asesores entendidos en el tema, y ser capaces de brindar sustento y respaldo legal para cada una de los delitos que se llegaran a cometer.
- Se debe tener una política de seguridad para cada institución, con el objetivo de introducir normas básicas o guiarse de textos, para el manejo de sistemas informáticos como también en su parte de telecomunicaciones.
- Se debe capacitar a todas las personas para que sean más atentas mediante charlas, conferencias entre otras para que no sean víctimas de este tipo de delitos y con esto precautelar la información que poseen dentro y fuera de sus lugares de trabajo y que no sean blanco fáciles de los delincuentes que comenten actos ilícitos.
- Dado el carácter trasnacional de los delitos informáticos y de telecomunicaciones, mediante el uso de las computadoras se hace imprescindible establecer tratados de extradición o acuerdos de ayuda mutua entre todos países, como también permitan fijar mecanismos para la cooperación internacional con el fin de contrarrestar eficazmente la incidencia de la criminalidad informática.

BIBLIOGRAFÍA

Acurio del Pino, D. S. (s.f.). Definición y el concepto de Delitos Informáticos. En *Delitos Informáticos* (págs. 10-11).

Acurio del Pino, S. (s.f.). Sujetos del delito informático. En *Delitos Informaticos* (págs. 15-20).

ALEGSA.COM.AR. (s.f.). *DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA*. (ALEGSA.COM.AR) Recuperado el 14 de Agosto de 2015, de http://www.alegsa.com.ar/Dic/control%20de%20acceso.php

Burnett, P., Trend Micro Incorporated, & OEA. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas.* Washington, D.C.,.

Diario EL COMERCIO. (20 de Julio de 2015). *Quien intercepte mensajes puede ser sancionado con 5 años de prisión*. Recuperado el 2 de Diciembre de 2015, de http://www.elcomercio.com/actualidad/interceptar-mensajes-presion-hackeo-ecuador.html

Fiscalia General del Estado del Ecuador. (13 de junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Recuperado el 2 de Diciembre de 2015, de Los delitos informáticos van desde el fraude hasta el espionaje: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Gercke, M. (2014). *Comprensión del Ciberdelito: FENÓMENOS, DIFICULTADES Y RESPUESTA JURÍDICA.* Ginebra.

Hacker, Cracker, Lammer, Newbie. (15 de Noviembre de 2009). Recuperado el 21 de Agosto de 2015, de http://planethacked.blogspot.com/2009/11/hacker-cracker-lammer-newbie.html

Informático, D. d. (s.f.). *DEFINICIÓN DE DELITO INFORMÁTICO*. Recuperado el 7 de Agosto de 2015, de http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Loredo González, J. A., & Ramírez Granados , A. (2013). *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo.* San Nicolás de los Garza, Nuevo León.

Meza Ayala, M. J. (2008). Fraude en Roming, Robo de líneas Telefónicas. En *Fraude en Telecomunicaciones.* Quito: Publiasesores.

Meza Ayala, M. J. (2008). *Fraudes en Telecomunicaciones.* Quito: Publiasesores.

mx, C. (s.f.). *Delitos informáticos*. Recuperado el 2 de Septiembre de 2015, de http://www.criminalistica.com.mx/areas-forenses/seguridad-publica/548-delitos-informcos

Pino, S. A. (s.f.). Tipos de Delitos Informáticos. En *Delitos Informáticos* (págs. 22-29).

Roldán, C. S. (s.f.). *Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?* (Codejobs) Recuperado el 12 de Agosto de 2015, de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.aB6Ne245.dpbs

Sarasola, I. (s.f.). *Que es cracker informatico*. Recuperado el 21 de Agosto de 2015, de http://cracker88.galeon.com/

Seguridad Informatica. (29 de Octubre de 2011). Recuperado el 15 de Agosto de 2015, de http://lyzzy-seguridadinformatica.blogspot.com/2011/10/unidad-3-control-de-acceso.html

Supertel. (2011). Clonación de teléfonos celulares, Call back o llamada revertida, By pass, Fraude Tercer País. *Delitos en telecomunicaciones 2011*, 4-6, 12-16.

Wikepedia. (s.f.). *Hacker (seguridad informática)*. (Wikepedia) Recuperado el 20 de Agosto de 2015, de https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)#Pandillas_criminales_organizadas

YADERSY. (31 de Julio de 2014). *Fases o Etapas de un ataque informático*. Recuperado el 28 de Agosto de 2015, de https://yadersy.wordpress.com/2014/07/31/fases-o-etapas-de-un-ataque-informatico/