FACULTAD DE INGENIERÍAS

CARRERA:

Ingeniería en Sistemas con Mención en Informática para la Gestión

Tesis previa a la Obtención del Título de:

INGENIERO DE SISTEMAS

TEMA

"Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos."

AUTORES:

Aracely del Rocío Cortez Díaz
Cindy Melina Chang Lascano

DIRECTOR:

Ing. Miguel Quiroz M.

Guayaquil - Ecuador
2012

DECLARATORIA DE RESPONSABILIDAD

Las ideas y contenidos expuestos en el presente trabajo académico, son de exclusiva responsabilidad de los autores.

Guayaquil, Julio del 2012

f……..
Aracely del Rocío Cortez Díaz

f……..
Cindy Melina Chang Lascano

D E D I C A T O R I A

A mi familia, a mis amigas y a cada una de las personas que de alguna forma han sido participes de este logro.

Aracely Cortez.

A Dios, a mi madre que siempre la llevare en mi corazón, a mi hija, a mi familia, a mis amigas y a las personas que en el transcurso de mi carrera me han brindado su apoyo para alcanzar esta meta.

Cindy Chang.

A G R A D E C I M I E N T O

A Dios por permitirme estar viva, a mi maravillosa familia que con su apoyo incondicional ha sido posible este logro. A mis amigas que siempre estuvieron cuando las necesite, a nuestro director de tesis que nos ayudó para la elaboración de la misma, y a cada uno de mis profesores por sus enseñanzas durante estos años en las aulas de clases.

Aracely Cortez.

Mi agradecimiento va principalmente para Dios, que me ha dado mucha fortaleza y me ha permitido levantarme muchas veces, a mi madre que desde el cielo sé que está muy orgullosa, a mis tías que han sido unas manos amigas que han estado como pilar fundamental para alcanzar este logro, a mi hija que es la razón de mis días , a mi esposo por sus palabras de aliento, a mis amigas las cuales he compartido mucho y han sido mi gran ayuda, a nuestro director de tesis, y a todos los docentes que estuvieron compartiendo sus conocimientos en el transcurso de mi carrera.

Cindy Chang.

ESQUEMA CAPITULAR

Índice General

Índice de Figuras

Índice de Tablas

Índice de Anexos

RESUMEN

CARRERA DE INGENIERÍA EN SISTEMAS

AÑO	ALUMNOS	DIRECTOR DE TESIS	TEMA TESIS
2012	ARACELY DEL ROCÍO CORTEZ DÍAZ CINDY MELINA CHANG LASCANO	ING. MIGUEL QUIROZ	"Diseño de nuevo esquema para el procedimiento de indagación de los delitos informáticos."

El presente tema de tesis tiene como objetivo establecer todas las formas de delito informático con herramientas tecnológicas, mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los mismos. Para confirmar las hipótesis planteadas se utilizo cuestionarios para medir el nivel de conocimiento a los involucrados en la administración de justicia, se realizo entrevista a persona experta sobre delitos informáticos. Para el análisis de la información se utilizo un software para tabular los datos y presentar información en forma gráfica. Se devela en las encuestas y entrevista la inexistencia de acciones procedimentales, planes bien establecidos para resolver los casos de delitos informáticos y la falta de conocimiento sobre herramientas para adquirir, preservar y recuperar evidencias digitales, además que los jueces no tienen adiestramiento para manejar estas evidencias. Lo cual confirma la importancia de la propuesta del Diseño de nuevo esquema para el procedimiento de indagación de los delitos informáticos, estableciendo los requerimientos mínimos necesarios para que la entidad pueda ejercer sus actividades de una manera eficiente, contando con funciones bien definidas según las necesidades actuales y con los recursos con los que se cuentan, estableciendo también procesos y procedimientos que permitan controlar las funciones y realizar monitoreo. La importancia científica de esta propuesta es la de aportar a la Administración de Justicia lineamientos que permitan planificar, motivar y gestionar rápidamente la indagación de delitos informáticos.

ABSTRACT

CAREER IN SYSTEMS ENGINEERING

YEAR	STUDENTS	THESIS DIRECTOR	THESIS TOPIC
2012	ARACELY DEL ROCÍO CORTEZ DÍAZ CINDY MELINA CHANG LASCANO	ENG. MIGUEL QUIROZ	"Design of new scheme for the investigation process of IT crime"

The current thesis topic has an objective to establish all forms of IT crime with technology tools, by designing a scheme that has procedures, functions and minimum requirements to attack them. To confirm the hypothesis proposed, surveys were used to measure the level of knowledge to the involved ones in Justice Administration, and interviews were done to people specialized in IT crime. For information analysis, software was used to tabulate the data and present information in graphical form. It reveals in surveys and interviews the lack of procedural actions, well-established plans for dealing with IT crime cases and the lack of knowledge about tools to acquire, preserve and recover digital evidences, moreover, that judges are not trained to handle these evidences. This confirms the importance of the proposal of new design scheme for the investigation process of IT crime, establishing the minimum necessary requirements for the entity to perform its activities efficiently, counting with well-defined functions according to current needs and the resources that they have, establishing processes and procedures that allow controlling functions and performing monitoring. The scientific importance of this proposal is to contribute to the Justice Administration guidelines for planning, motivating and quickly handle the investigation of IT crime.

INTRODUCCIÓN

El presente proyecto de tesis es una propuesta que sirve para poder implementar un nuevo esquema para el procedimiento de indagación de los delitos informáticos, en conjunto con las regulaciones existentes (leyes) para el manejo de los mismos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los criterios y medidas contempladas.

Haciendo conocer cada uno de los proceso y funciones de cada uno de los participantes en la indagación de los delitos informáticos**,** y que estos puedan resolverlos de una manera ágil y precisa. Que cuenten con la preparación y pericia requerida para identificar, recoger, analizar, y reportar evidencia digital como participantes en la Administración de Justicia en la Sociedad Ecuatoriana.

Este trabajo está dividido en 5 capítulos:

En el Capítulo 1, se revisa el planteamiento del problema, presentando la situación actual de la administración de justicia, la justificación y objetivos de la investigación.

En el Capítulo 2, se describe el concepto y clasificación del delito informático, el perfil del especialista en la administración de justicia en la sociedad ecuatoriana, formulación de hipótesis y variable de acuerdo a la información obtenida.

En el Capítulo 3, se detalla la metodología de investigación realizada para obtener la información y los mecanismos para el tratamiento de la misma.

En el Capítulo 4, se detalla cómo se analiza la información y la interpretación de los resultados. Se verifican las hipótesis planteadas.

En el Capítulo 5, se presenta el manual de procesos, funciones y requerimientos mínimos para indagar y resolver los delitos informáticos, se muestra ejemplos de delitos informáticos.

CAPÍTULO 1

DISEÑO DE LA INVESTIGACIÓN

1.1 Antecedentes de la Investigación

Muchas personas se han dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras tratan de utilizar la tecnología, las computadoras y sistemas, para el cumplimiento de actividades ilícitas.

Empresas de toda índole y a nivel Mundial han sido perjudicadas por esta clase de delitos que a menudo son personas que están inmersas en el campo de la informática y con elevadas posibilidades de que no lleguen a descubrirles. Por lo tanto, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyon, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet. El "Grupo de Lyon" utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.

Al mismo tiempo, y guiado por los participantes en el grupo de Lyon, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el "delito informático".

En la actualidad el uso de la red mundial de información permite realizar negocios por vía telemática, realizar transferencias de fondos y utilización de datos en forma rápida, casi inmediata. Este desarrollo permite que también aparezcan nuevas formas

de delinquir. Los perjudicados estafados por usar los servicios informáticos de las instituciones acusan a éstas de no tener las suficientes seguridades informáticas en sus páginas web.

Nuestra legislación se basa en el principio del Derecho Romano: "nulliun crimen nullium pena sine lege", precepto que se consagra en la ley del Ecuador, de que no existe delito si previamente no se encuentra determinada la conducta típica antijurídica en la ley, por tanto, en nuestro país no existe ley del delito informático propiamente dicho.

La Fiscalía registra entre el año 2010 y abril del 2011 2.006 robos informáticos. Explica que la "institución, al omitir su deber de protección, no le informa al cliente de los riesgos que existen al usar el servicio de banca en línea".

Las instituciones bancarias, son las mayores afectadas, según indagación de la Fiscalía.

Según experto de la fiscalía, el total en robos realizados por internet llega a $ 3 millones, de los que se debería recuperar el 80% (aproximadamente $ 2,4 millones).

El fiscal especifica que entre las instituciones bancarias el 80% de los robos fue menor a $ 2 mil, el 15% menor a $ 10 mil y el restante 5% superior a $ 10 mil.

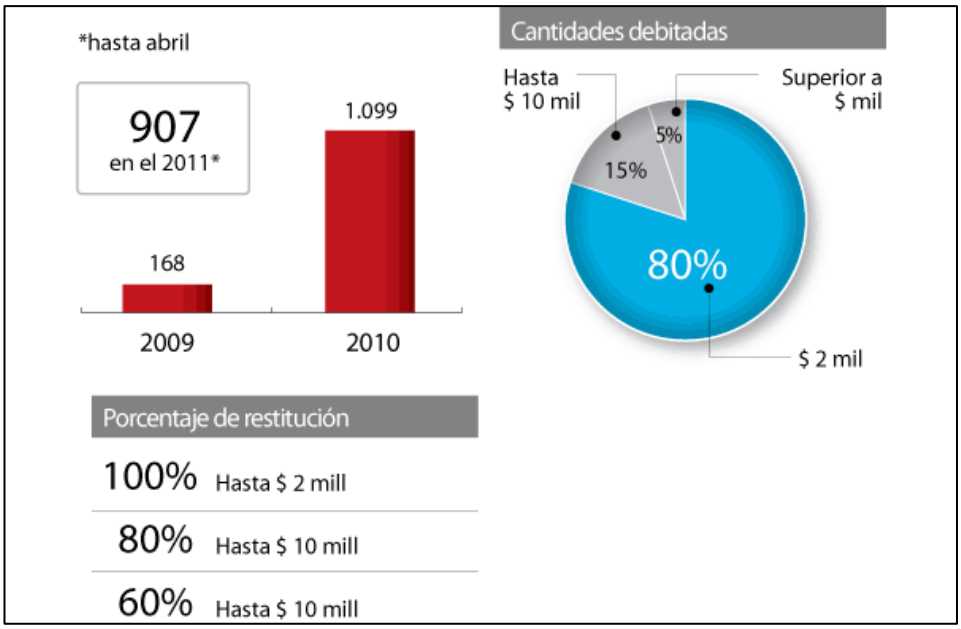


Figura 1.1 Delitos por Internet

Fuente: Fiscalia General y Superintendencia de Bancos, 2010

La falta de una política o un diseño efectivo en cuanto al uso de las TICS, seguirá generando aumento en los casos de robos informáticos, por lo que los servicios informáticos no cuentan con la suficiente protección, para brindar seguridad a sus usuarios.

El desarrollo de las nuevas tecnologías de la información y de la comunicación se quedará interrumpido, por la resistencia de las personas a usar los servicios informáticos, que en otros países son usados diariamente.

1.2 Problema de Investigación

1.2.1 Planteamiento del Problema

Pese a que existe una ley desde el 2002, en la que se tipifican algunas formas de delitos informáticos como: fraudes, acceso no acreditado a sistemas de información, daños informáticos, etc., es necesaria la creación de la Ley de Delito Informático para definir nuevos tipos penales y mejorar la legislación para combatir otras formas del delito en esta área.

Tanto la Fiscalía como la Policía han hecho esfuerzos para capacitar a su personal sobre esta forma de delinquir, pero aún no poseen herramientas para adquirir, preservar y recuperar evidencias digitales. Además, los jueces deben tener un mayor adiestramiento para manejar estas evidencias que no son físicas sino intangibles.

Actualmente no existe una seguridad total para el usuario debido al enorme campo que incluye el mundo virtual. Para minimizar los efectos de este tipo de delitos lo importante es prevenir, mediante la educación sobre temas de seguridad, y sancionar a través de normas legales que castiguen específicamente este tipo de actos delictivos.

Los 2.006 casos de robos informáticos entre el año del 2010 y abril del 2011.Muestra la falta de una política criminal articulada en cuanto al uso de tecnologías, y la de un nivel de conocimiento aceptable de las TICS por parte de las instituciones que ofrecen servicios informáticos.

Ilícitos como la clonación de tarjetas de crédito y débito, suplantación de identidad por internet o por teléfono, los 'troyanos bancarios' y documentos han aumentado en el país en los últimos años, en la misma medida en que ha disminuido la brecha tecnológica, es decir, el acceso de la ciudadanía a herramientas como internet.

Si no se cuenta con procedimientos y conocimientos claros en cuanto a la prevención y juzgamiento de los delitos informáticos, van a seguir en aumento los casos de estos. Ya que no se resuelven a tiempo y con éxito. El desarrollo de las nuevas tecnologías de la información y de la comunicación se quedará interrumpido, por la resistencia de las personas a usar los servicios informáticos, que en otros países son usados diariamente.

Para superar este problema, ya sea porque la gente no denuncia o porque no existe la tipificación de un delito, la sociedad debe denunciar y el Estado garantizar mecanismos estadísticos y de juzgamiento.

La propuesta surge como factor incluyente para cada uno de los involucrados que dirigen la investigación pericial tecnológica, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos.
Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático (Ministerio Publico, Policía Judicial, jueces, etc.).

Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas.

Falta de cultura informática, aquellos individuos que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito[1].

Contexto

El presente proyecto tiene como objetivo identificar los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana para el tratamiento de los mismos.

Se abordará el marco conceptual de los delitos y la criminalidad informática, así como también las leyes relacionadas que se encuentran establecidas en la legislación ecuatoriana.

Se observará los retos a nivel de formación, limitaciones tecnológicas, el marco legal que la Administración de Justicia en la Sociedad Ecuatoriana debe superar para hacer frente a estas conductas delictivas que hacen uso de las nuevas tecnologías.

[1] **Plan Operativo Unidad de Delitos Informático, Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito, 2010**

1.2.1.1 Situación - Conflicto

1.2.1.1.1 Situación Actual de la Administración de Justicia en Guayaquil

Lo primero que sorprende a cualquier analista de nuestro sistema de administración de justicia es, posiblemente, el enorme retraso que esta parte de nuestra administración pública ofrece frente al resto del sector público. Configurada tradicionalmente como una suerte de administración pública singular, individualizada por su función y, sobre todo, por el estatuto jurídico del personal a su servicio, lo cierto es que la administración de justicia ha caminado tradicionalmente con unas dosis muy fuertes de autonomía frente al resto de administraciones públicas, autonomía que se ha venido justificando en que al fin y a la postre esa administración era el instrumento de gestión de un poder judicial. En todo este proceso de individualización de la administración de justicia ha jugado, una vez más, un papel determinante la evolución histórica, o si se prefiere nuestras tradiciones. Porque en honor a la verdad del texto constitucional no se puede derivar con claridad meridiana que a la administración de justicia no le sean de aplicación los principios y reglas constitucionales predicables de la administración pública en general. Bien es cierto que en la Constitución se recoge una reserva específica a un tipo concreto de ley orgánica (la ley orgánica del poder judicial) que será la que deba determinar "la constitución, funcionamiento y Gobierno de los Juzgados y Tribunales, así como el estatuto de Jueces y Tribunales, que formarán un Cuerpo único, y del personal al servicio de la administración de justicia"[2]

No es, efectivamente, la única referencia que la Constitución hace a la "Administración de Justicia", pero sí es en verdad la más certera (o, al menos, la más precisa) en cuanto a su alcance.

Pues en otros pasajes el texto constitucional lleva a cabo una referencia a la administración de justicia vinculada con la idea de "administrar" o "impartir" justicia, muy apegada por tanto a las influencias del proceso revolucionario francés que configuró una de justicia meramente aplicativa de la ley, donde el juez se

[2] **Código de Procedimiento Civil, Quito, 2009**

limitaba a “administrar” (esto es, a aplicar mecánicamente) la voluntad previamente fijada por el legislador, en lo que fue una traslación más o menos fiel de esa concepción del poder judicial de Montesquieu como “poder neutro”, que se manifestaba en esa definición de los jueces como “seres inanimados que no pueden moderar ni la fuerza ni el rigor de las leyes”.

Dicho en otros términos, las referencias constitucionales a la administración de justicia en sentido estricto son, en nuestra Constitución, ciertamente parcas y hasta se podría decir que a todas luces insuficientes, lo que contrasta evidentemente con la mayor precisión que alcanzan los principios y reglas constitucionales relativos a la administración pública como ente instrumental del Ejecutivo. Pero esas escasas referencias no pueden conducir al equívoco de que a la administración de justicia no le son aplicables al menos los principios recogidos en el texto constitucional y predicable de la administración pública en su conjunto.

En efecto, ha costado muchos años asentar en Ecuador la idea fuerza de que la Justicia, aparte de ser evidentemente un poder del Estado, es además un servicio público. De hecho, se puede decir que hasta la aprobación de la nueva constitución tal idea no consigue cuajar de modo efectivo. A partir de ese momento, y no sin dificultades, se asienta entre nosotros una necesidad objetiva que consiste claramente en que la administración de justicia debe funcionar de acuerdo con los principios de eficacia y eficiencia, por tanto racionalmente, y en consecuencia debe adaptar sus estructuras y su organización a parámetros de actuación que ya estaban presentes por lo demás en el resto de administraciones públicas.

En fin, en este rápido recorrido se ha podido constatar que ni siquiera en el plano normativo, la administración de justicia se ha ido adaptando al cambio exigido por el desarrollo de las nuevas tecnologías de la información y de la comunicación.

Sería ingenuo por nuestra parte no dejar constancia de que todavía hoy las cuestiones normativas en este campo se siguen moviendo más en un terreno propio de los deseos incumplidos. Cualquier mínimo conocedor de la realidad de la administración de justicia en Ecuador es plenamente consciente del déficit que todavía hoy ese proceso presenta. En este punto, a pesar de los avances, que los ha habido, la

distancia con otros sectores de lo público siguen siendo considerables.

Es preciso evaluar si las aplicaciones permiten realizar estos cometidos y también la utilización que de ellas hacen los usuarios; es obvio, por tanto, que en este campo de la informatización de la administración de justicia el camino recorrido ha sido mínimo. Se debe realizar un esfuerzo inversor y fomentar el uso de las nuevas tecnologías en el espacio interno de la administración de justicia. Mejorar instrumentos de comunicación y de obtención de información.

Esto se debe en gran medida a la falta de uso de las TICS en las Universidades y facultades de Derecho, donde se ha dejado de lado la Tecnología y no se ha avanzado en la preparación del Profesional que administra justicia, peor aún estar preparados para los cambios que la Administración de Justicia en la Sociedad incurre y por lo tanto de actividades delictivas en la ciudad.

1.2.1.1.1 Situación Actual del Delito Informático en la Administración de Justicia en la Sociedad (Guayaquil)

El medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorción, robo, fraude, suplantación de identidad, entre otros.

La delincuencia informática es difícil de comprender o conceptualizar plenamente, a menudo se la considera una conducta relegada por la legislación, que implica la utilización de tecnologías para la comisión del delito.

La investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta. Es preciso considerar que el internet brinda grandes beneficios a los usuarios, pero su fácil acceso también podría perjudicarlos.

Según las estadísticas del mes de Septiembre del 2008, de la Superintendencia de Telecomunicaciones en Ecuador, hay alrededor de 1´329.713 usuarios de Internet, los cuales corren un alto riesgo de ser perjudicados mediante actos delictivos como la

ingeniería social, estafa, un ataque de phishing u otros, relacionados con las tecnologías.

Las cifras sobre los delitos informáticos, en Ecuador también son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos.

Es importante considerar los retos particulares que están latentes a todo nivel e incluso para los actores involucrados, en el manejo de los Delitos Informáticos, sean estos el Ministerio Público, la Policía Judicial, la Corte de Justicia, investigadores, y hasta la misma sociedad.

Las Necesidades de la Administración de Justicia en la Sociedad ecuatoriana se basa en la realidad de la situación que existe en las administraciones de justicia debido a la falta de conocimiento en la parte informática, donde existen diversos delito, y no hay la información necesaria para diagnosticar el debido delito y por ende la sanción por esta.

- Tener profesionales en Derecho que tengan conocimiento en la parte informática, para que con su sustento legal puedan analizar debidamente este tipo de delitos como son los informáticos.

Las Necesidades del profesional que se necesita en la Administración de Justicia en la Sociedad ecuatoriana en el marco de la criminalidad informática:

- Diferenciar los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

- Tener especialistas académicos y no empíricos en el tratamiento de los delitos informáticos.

- Tener un esquema para el procedimiento de indagación de los delitos informáticos. Causas del Problema, Consecuencias.

1.2.1.2 Árbol de Problemas

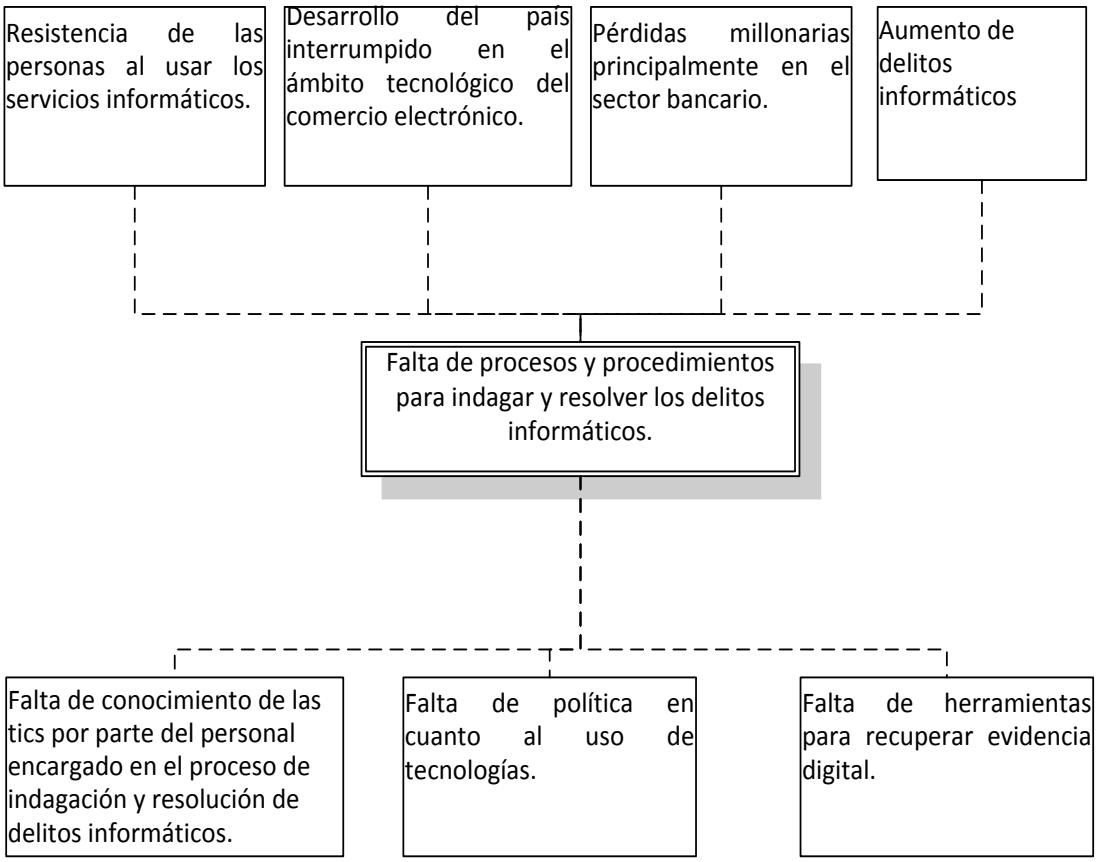


Figura 1.2 Árbol de Problemas

Fuente: Autores

La entidad encargada de la indagación y resolución de delitos informáticos no cuenta con el suficiente conocimiento de las tics. La ausencia de una política bien establecida en cuanto a su uso. Y la falta de herramientas para recuperar la evidencia digital. Impiden que la entidad cuente con procesos y procedimientos que faciliten la indagación y resolución de delitos informáticos. Causando que los delitos informáticos estén en aumento, pérdidas millonarias principalmente en el sector bancario, resistencia de las personas al usar los servicios informáticos, impidiendo el desarrollo tecnológico del país.

1.2.2 Formulación del Problema

¿Cuáles son las acciones procedimentales y recolección de evidencias a seguir contra los Delitos Informáticos en el Ecuador?

Causas

El cambio en el entorno social y el crecimiento constante de la tecnología, es profundo: las relaciones de la tecnología en la Administración de Justicia en la Sociedad de un modo radical, y se encuentran frente a actividades que no sólo tienen incidencia directa en la sociedad, sino que, a diferencia de otros actos delictivos no se tiene profesionales especializados en la temática, no se está preparado sensiblemente para entender y responder a los mismos.

Al establecer nuestro problema como la falta de procesos y procedimiento para indagar y resolver los delitos informáticos en cuyas causas va:

La entidad encargada de la indagación y resolución de delitos informáticos no cuentan con el suficiente conocimiento de las tics. Ausencia de una política bien establecida en cuanto a su uso. Y falta de herramientas para recuperar la evidencia digital.

Consecuencias

En la Administración de Justicia en la Sociedad Ecuatoriana se cuenta con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Unidad de Delitos Informáticos de la Fiscalía General del Estado, creada en 1990.

Pese a estos y otros esfuerzos, las autoridades aún afrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos para que se les siga

juicio en otro lugar o transferir las pruebas y a veces los testigos al lugar donde se cometieron los delitos, sumidos al problema de establecer la jurisdicción y competencia.

A continuación se detallan bajo este contexto algunos inconvenientes para el manejo de delitos informáticos por la falta de especialistas en la rama:

Falta de la infraestructura y tecnologías adecuada en los entes u organismos de la Administración de Justicia en investigación como: el Ministerio Público y la Policía Judicial. Las investigaciones o experticias a nivel informático en su mayoría se dan por denuncias realizadas bajo otro contexto de delitos tales como: robo, daño a la propiedad, estafas, entre otros, que son llevadas por Unidades del Ministerio Público como: la Unidad de Delitos Misceláneos, Unidad de Delitos Financieros y de Telecomunicaciones, Unidad de Daños contra la Propiedad, debido a la falta de una regulación, o unidad que opere este tipo de infracciones.

Falta de iniciativas que permitan el desarrollo de brigadas y unidades estructuradas y especializadas, para la investigación de los delitos de índole informático, nacional y transnacional, desde su inicio con el levantamiento de evidencias hasta la aplicación de procedimientos de mayor complejidad.

Falta de especificaciones claras y concisas en la petición de pericias informáticas, elemento importante que cabe destacar, ya que durante las peticiones de pericias informáticas solicitadas por medio de la autoridad, incurre en términos amplios sobre la “práctica de peritaje informático”, en la cual no se especifican requerimientos sólidos sobre lo que se va a investigar, en cuyo caso es importante la comunicación entre los fiscales, jueces y tribunales con los investigadores o peritos de la rama de informática, previo a establecer la diligencia de la pericia.

Falta de una comunicación efectiva entre los especialista informáticos y los judiciales; mantener un lenguaje común entre los especialistas de informática y los operadores judiciales es trascendental, principalmente, al exponer por parte del perito informático, los criterios utilizados en el desarrollo de la investigación ante una investigación judicial.

Falta de un procedimiento adecuado para la calificación de peritos informáticos por parte del Ministerio Público y demás entidades u organismos.

Otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

Lo que hace que los delitos informáticos estén en aumento, pérdidas millonarias principalmente en el sector bancario, resistencia de las personas al usar los servicios informáticos, impidiendo el desarrollo tecnológico del país.

Delimitación del Problema

Campo: Administración de Justicia – Criminalidad Informática

La Criminalidad Informática en la Administración de Justicia comprende la Gestión de Justicia de cualquier comportamiento criminógeno, en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como un simple símbolo", entonces según esta descripción las personas que cometen delitos o crímenes informáticos, están enmarcadas dentro de lo que se conoce como criminología, y la investigación de dichos delitos, están sujetos a las ciencias de la criminalística.

Es preciso que se reconozca la diferencia entre la criminología y la criminalística; La criminología trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística se definen como los conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen" , la criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, y se apoya de métodos y técnicas propias del trabajo de las diferentes disciplinas.

Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos

informáticos, ya que han tenido un repunte a los largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

El informe de Evolución de Incidentes de Seguridad que corresponde al año 2010, elaborado anualmente desde 1999 por la Fiscalía General del Estado determina que el incremento de incidentes que ha habido entre el año 2006 al 2010 es el 63.32% en el que se involucran escaneo de puertos en busca de equipos vulnerables, vulnerabilidades de sistemas web, errores de programación, vulnerabilidades de navegadores más utilizados, ataques de phishing, máquinas zombis, malware y otro tipo de ataques para el cometimiento de fraudes u inhabilitación de servicios, este mismo informe indica que el patrón de ataque continua siendo más dirigido, inteligente y silencioso con algún tipo de trasfondo que puede ser económico, religiosos, político o de ansias de poder.

Otro organismo que realiza investigaciones de este nivel es la Unidad de Delitos Informáticos, que publica una variedad de estadísticas relacionadas con las vulnerabilidades, que se han catalogado basados en informes de fuentes públicas y reportes que son directamente comunicados mediante su sistemas web. Tal como se puede observar, se concluye que la tendencia sobre las vulnerabilidades tiene un crecimiento significativo a lo largo de los años que se han analizado.[3]

La criminalidad informática organizada ha crecido de manera exponencial, de acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades reportadas y los altos costos que estos involucran para la empresa y el estado, los mismos, que son aprovechadas por los intrusos, cabe recalcar dichos intrusos conocen cada vez con más profundidad los detalles de las tecnologías y sus limitaciones, por ello, es cada vez más fácil desaparecer la evidencia y confundir a los investigadores, por lo cual, constituye un reto para los sectores afectados, los legisladores, judiciales, policiales e incluso los especialistas informáticos encargados de su investigación.

3 Informe de Evolución de Incidentes Tecnológicos , Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito,2009

Área: Ingeniería (Tecnología-Sistemas) para la Administración de Justicia

Con el advenimiento de las nuevas tecnologías, la sensación de mutación y cambio tecnológico se ha hecho más palpable y con ello la importancia de la ingeniería en las decisiones de la sociedad. Las nuevas tecnologías están en la base de una economía global o "economía informacional", caracterizada porque la productividad y la competitividad se basan de forma creciente en la generación de nuevos conocimientos y en el acceso a la información adecuada, bajo nuevas formas organizativas que atienden una demanda mundial cambiante y unos valores culturales versátiles.

Este nuevo sistema tecno-científico que implica un nuevo paradigma tecno económico, se caracteriza por una nueva forma que depende en gran medida de una serie de innovaciones tecnológicas. La construcción y el funcionamiento de cada uno de esos artefactos presuponen numerosos conocimientos científicos y tecnológicos (electricidad, electrónica, informática, transistorización, digitalización, óptica, compresión, criptología, etc.).

Estamos ante una transformación de mayor entidad basada en un nuevo espacio de interacción entre los seres humanos, en el que surgen nuevas formas sociales y se modifican muchas de las formas anteriores. Se está modificando profundamente la vida social, tanto en los ámbitos públicos como en los privados, el sistema tecno científico incide sobre la producción, el trabajo, el comercio, el dinero, la escritura, la identidad personal, la noción de territorio, memoria y también sobre la política, la ciencia, la información y las comunicaciones y la educación.

Aspecto: Falta de Conocimiento de las TICS en la Administración de Justicia

Surge como factor incluyente para cada uno de los involucrados que dirigen la investigación en la Administración de Justicia, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos.

- Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático (Ministerio Publico, Policía Judicial, jueces, etc.).

- Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas.

- Falta de cultura informática, aquellos individuos que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

Ecuador no ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sobre todo en las áreas involucradas directamente, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación.

Luego de analizar la realidad de los delitos informáticos en la Administración de Justicia en el Ecuador y exponer mecanismos y herramientas existentes para su investigación, se realizará el diseño de nuevo esquema para el procedimiento de indagación de los delitos informáticos, que se espera sea considerado por los diferentes sectores: Gubernamental, Marco Legal, formación, tecnología y sociedad.

Evaluación del Problema

El cambio en el entorno social y el crecimiento constante de la tecnología, es profundo: las relaciones de la tecnología en la Administración de Justicia en la Sociedad de un modo radical, y se encuentran frente a actividades que no sólo tienen incidencia directa en la sociedad.

Problema:

- Falta de preparación para los miembros de los organismos de la Administración de Justicia que persiguen la delincuencia en el campo informático (Ministerio Publico, Policía Judicial, jueces, abogados en libre ejercicio, etc.).

- Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas de la Administración de Justicia en la Sociedad Ecuatoriana.

- Falta de programas de capacitación que atañen a los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana.

- Falta de cultura informática en la sociedad, aquellos individuos que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

Determinación de las Causas

Que el Estado a través de las Instituciones administradoras de justicia no se encuentre actualizado de acuerdo a las nuevas tendencias tecnológicas depende de una serie de razones y es importante que en la institución se conozcan las causas específicas a fin de adoptar medidas de corrección para evitar que el problema se repita en el futuro. A continuación se ilustran algunas de las posibles causas.

Falta de Planes / Programas / Estrategias de Capacitación en la Administración de Justicia

- Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Abogados) sobre los delitos informáticos y la informática legal.

- Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc en la Administración de Justicia en la Sociedad Ecuatoriana.

- Fomentar el desarrollo de programas que involucren la disertación del peritaje informático, legislación existente que atañen a la informática, criminalística en la Administración de Justicia en la Sociedad Ecuatoriana.

Falta de Interés en la Sociedad

- Advertir a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos.

- Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico.

- Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos.

- Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.

Falta de Intervención y Asignación de Recursos del Estado

- Convenios institucionales (universidades, gremios, etc.).

- Cooperación y transferencia de conocimiento con países vecinos, o con quienes se hayan establecido convenios internacionales, sobre la tecnología existente o el desarrollo de las mismas que permitan la persecución de los delitos informáticos.

- Implementación de laboratorios especializados forenses informáticos.

1.2.3 Sistematización del Problema

- ¿Cuáles son los mecanismos estadísticos y de juzgamiento empleados por el estado para resolver los delitos informáticos?

- ¿Dónde se dirigen las personas afectadas por los delitos informáticos?

- ¿Cuentan los jueces con una visión clara sobre los delitos informáticos?

- ¿Cuentan con procedimientos y planes de acción para regular los delitos informáticos?

- ¿Cómo se podría reducir los casos de delitos informáticos?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Establecer todas las formas de delito informático con herramientas tecnológicas mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los delitos informáticos.

1.3.2 Objetivos Específicos

- Establecer mecanismos procedimentales y de juzgamiento para ayudar a resolver los delitos informáticos.

- Proponer funciones y requisitos mínimos para personal especializado en resolver los delitos informáticos.

- Establecer las características, parametrizar, encasillar los delitos informáticos.

- Identificar los procedimientos y planes de acción para regular los delitos informáticos

- Identificar y analizar soluciones para reducir los casos de delitos informáticos.

1.4 Justificación de la Investigación

Los delitos informáticos han causado ingentes pérdidas económicas, a lo que se suma la pérdida de credibilidad y debilitamiento institucional que sufren las entidades afectadas, especialmente en el sector comercial y bancario donde por ejemplo las manipulaciones informáticas fraudulentas ganan terreno cada vez más. Al ser evidente la fragilidad tecnológica en las entidades se refleja la importancia de nuestra investigación al querer demostrar los problemas en el Ecuador en cuanto al uso de las TICS en las mismas y como los organismos de control hacen frente a los delitos informáticos. Luego de los resultados de la investigación se quiere desarrollar un esquema que estandarice en cuanto a un mejor uso de las TICS, para prevenir de una manera eficaz los delitos informáticos y resolver rápidamente los mismos.

La estandarización consiste en un diseño de las mejores Tics en cuanto a especificaciones de hardware, software, procedimientos, políticas, técnicas, para prevenir los delitos informáticos en los portales. Basándonos en tecnologías de la actualidad y la facilidad de acceso en nuestro país. Tomando como referencia a países desarrollados como Estados Unidos, Alemania, etc. Todo esto con el fin de que las entidades mejoren la seguridad de sus servicios informáticos para que las personas los usen y así seguir avanzando con el desarrollo tecnológico del país.

El diseño también abarca un nuevo esquema para el proceso de indagación de delitos informáticos para poder resolver rápidamente los mismos. Mediante el establecimiento de un plan estratégico de capacitación al personal encargado de la Gestión de Justicia, Peritos/Especialistas Informáticos. Brindando una visión global del estado de los delitos informáticos en el Ecuador, identificando claramente los retos y brechas que deben ser superadas para el tratamiento de los mismos.

Según cifras de la Fiscalía, existen, desde enero de 2010 a la fecha, alrededor de 2000 personas que han sido perjudicadas económicamente a través de transferencias electrónicas.

Casos como; Estafas / Suplantación de identidad, Infracciones de Propiedad Intelectual, Clonación de Tarjetas, etc. Demuestra la falta de un esquema que permita

utilizar de una mejor manera las TICS.

Los principales fundamentos que justifican la realización de este proyecto son:

- Contar con estándar con especificaciones detalladas de cómo prevenir los delitos informáticos, y como resolverlos más ágilmente.

- Incremento de la credibilidad del estado y de las entidades, principalmente de la comercial y bancaria. Al contar con un esquema que responda a las necesidades actuales.

- Elaboración de un proceso claro y específico para el procedimiento de indagación en este tipo de actividad delictiva.

Beneficios

Los elementos de prueba dentro de un proceso son de vital importancia, ya que mediante su investigación se llega a determinar la confirmación o desvirtuación de lo que corresponde a la verdad. Es trascendental, tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, ante un hecho de delito informático. El principal beneficiado es la Administración de Justicia en la Sociedad ya que se asegura que la administración de justicia en este tipo de delitos establezca justicia de acuerdo al marco legal del país.

Involucrados en el Proyecto: véase Anexo A
Análisis FODA del Proyecto: véase Anexo B
Marco Lógico del Proyecto: véase Anexo C

CAPITULO 2

MARCO DE REFERENCIA DE LA INVESTIGACIÓN

2.1 Marco Teórico

2.1.1 Delito

El delito es toda acción u omisión voluntaria penada por la ley. Esta definición está contenida en el artículo 1º del Código Penal. En forma simple, es la comisión de un hecho que la ley castiga con una cierta pena. Lo que hace característico al delito, es la existencia de una norma jurídica que debe haber sido dictada con anterioridad al hecho, que amenace fija una sanción al que realiza el hecho. Es decir previene la conducta por la amenaza de la sanción, y no por la prohibición. La ley no prohíbe robar, pero sanciona el robo con penas privativas de libertad. Además de la norma previa, el delito contiene una conducta típica, es decir la definición del hecho que la norma quiere impedir. "El empleado público que tenga a su cargo fondos públicos...". Este tipo dice que se aplicará la norma, sólo al empleado público, pero que además tenga a su cargo, es decir bajo su responsabilidad "fondos públicos". Por eso se dice que la conducta normada, debe caber exactamente en el hecho cometido, ya que si no calza perfectamente, no es ese el tipo penal aplicable.

Los delitos pueden clasificarse en: Crímenes, simples delitos y faltas. Una vez que se averigua que la persona ha cometido un delito y se sabe la pena que la ley aplica a ese ilícito, el juez deberá compensar entre las atenuantes de responsabilidad penal y las agravantes de responsabilidad penal. [4]

2.1.1.1 Clasificación del Delito

Por su Gravedad: tripartito y bipartito.

[4] **Roberto Alfredo González Maldonado - INFOIUS Ltda. , Diccionario Jurídico Chileno, 2001, www.juicios.cl**

El Sistema Tripartito divide en crímenes, delitos, contravenciones. Permite la individualización, la sociedad reacciona con mayor intensidad a los crímenes y es de utilidad práctica: determina la competencia de los tribunales, el jurado conoce los crímenes, las correccionales los delitos y la policía las contravenciones. Critica. No hay diferencia cualitativa entre crimen y delito, una lesión puede ser ambas, según la menor o mayor gravedad de sus consecuencias. [5]

El Sistema Bipartito divide en delitos y contravenciones. Se basa en la de la pena y la jurisdicción. Las diferencias entre delito y contravención serían: en el delito el daño es efectivo, en la contravención es un simple peligro; en el delito hay intensión manifiesta, en la contravención no hay mala intensión; el delito está en el código penal, la contravención esta en disposiciones especiales de caza, de pesca, en disposiciones sanitarias, etc.

Por la Forma de la Acción: de comisión, de omisión, de comisión por omisión. El delito de comisión viola ley prohibitiva, ej. , Robo, calumnia, aborto. El de omisión vulnera norma imperativa, ej. , Abandono de servicios.

Por la Forma de Ejecución: instantáneo, permanente, continuado, flagrante, conexo o compuesto.

Delito instantáneo. Aquel en que la violación jurídica realizada en el momento de consumación se extingue con esta. La acción coincide con la consumación.

El agente no tiene ningún poder para prolongarlo ni para hacerlo cesar. Ej. , En el homicidio, robo, hurto.

Delito Permanente. Después de la consumación continúa ininterrumpidamente la violación jurídica perfeccionada en aquella. Ej. , El rapto, el abandono de familia.

Delito Continuado. La acción implica una serie de violaciones jurídicas que tienden a un único resultado. La ley no da relevancia a estos actos (sí fuera así, serían varios

[5] **Jorge Machicado, Margot Mariaca , Ermo Quisbert, Clasificación del delito, 2007, www.enj.org**

delitos) Ej.: cajero que saca centavo a centavo hasta reunir una suma considerable. Delito Flagrante. Es el que se ha consumado públicamente y cuyo perpetrador ha sido visto por muchos testigos al tiempo en que lo cometía.

Delito Conexo. Las acciones están vinculadas de tal manera que unos resultados dependen de unas acciones y otros resultados de otras acciones. Ej., Los delincuentes se ponen de acuerdo antes, luego cometen delitos en diferentes tiempos y lugares.

Por las Consecuencias de la Acción: formal, material.

Delito formal (o de simple actividad), es aquel en que la ley no exige, para considerarlo consumado, los resultados buscados por el agente; basta el cumplimiento de hechos conducentes a esos resultados y el peligro de que estos se produzcan o basta también la sola manifestación de la voluntad. En los delitos formales jamás se da la Tentativa, este sólo se da en los delitos materiales.

Delito material (o de resultado) es el que se consuma mediante la producción de un daño efectivo que el delincuente se propone. El acto produce un resultado. Ej., el asesinato, el resultado de la acción es la muerte de una persona. En el robo, el resultado es la aprehensión de la cosa.

Por la Calidad del Sujeto: impropio, propio.

Delito Impropio es el realizado por cualquier persona.

Delito propio es aquel cometido por personas que reúnen ciertas condiciones relacionadas con el cargo público, oficio o profesión.

Por la Forma Procesal: de acción privada, de acción pública a instancia de parte, de acción pública.

Delito de acción privada. Se enjuicia y se persigue sólo a querella de parte ofendida, por ejemplo giro de cheque en descubierto, despojo, los delitos contra el honor (difamación e injuria).

Delito de Acción Pública a Instancia de parte. Aquel en que el Fiscal puede perseguir sólo ha pedido de la parte damnificada u ofendida. Ej. ,
Abandono de familia, de mujer embarazada…proxenetismo.

Delito de acción pública. Puede demandar quienquiera incluso el Ministerio Público de oficio. Ej. , El homicidio [6]

Por las Formas de Culpabilidad: doloso, culposo.

Delito doloso. Ejecución de un acto típicamente antijurídico con conocimiento y voluntad de la realización el resultado. No exige un saber jurídico, basta que sepa que su conducta es contraria al Derecho, peor aún, basta la intensión de cometer el hecho delictivo.

Delito culposo. "Un delito es Culposo cuando quien no observa el cuidado a que está obligado conforme a las circunstancias y sus condiciones personales y, por ello no toma conciencia de que realiza un tipo penal, y si lo toma, lo realiza en la confianza de que lo evitará". El delito es culposo cuando el resultado, aunque haya sido previsto; no ha sido querido por el agente pero sobreviene por imprudencia, negligencia o inobservancia de las leyes, reglamentos, órdenes, etc. Ej. , Fumar en surtidor de gasolina o exceso de velocidad que causan un accidente.

En el delito doloso existe intensión; en el delito culposo existe negligencia. En los delitos dolosos, para consumar la figura delictual, es necesaria la intensión de producir un resultado dañoso; en los delitos culposos basta con que ese resultado haya sido previsto o, al menos, que haya debido preverse.

Por la Relación Psíquica entre Sujeto y su Acto: preterintencional o ultraintencional.

Delito Preterintencional. (O ultraintencional) Es aquella, en que se desea cometer un delito pero resulta otro más grave. Ej. , Cuando sólo se lo quiere lesionar pero lo

[6] **Jorge Machicado, Margot Mariaca , Ermo Quisbert, Clasificación del delito, 2007, www.enj.org**

mata. La sanción sigue la Teoría de la Responsabilidad.

Objetiva, o sea, son calificados por el resultado, por el evento ocurrido, que no estaba en la intensión del agente.

Por El Numero De Personas: individual, colectivo Delitos Individuales. Son los realizados por una sola persona, ej. , La violación, el prevaricato.

Delitos Colectivos. Son los realizados por 2 o más personas ej. , Sedición, conspiración.

Por el Bien Vulnerado: simple, complejo, conexo

Delito Simple. Violan un solo bien o interés jurídicamente protegido, ej. , El homicidio viola el derecho a la vida. [7]

Delito Complejo. Violación de varios bienes o intereses protegidos. Ej. , Rapto seguido de violación. Es casi igual al Concurso Real De Delitos.

Delito Conexo. Las acciones están vinculadas de tal manera que unos resultados dependen de unas acciones y otros resultados de otras acciones. Ej. , Los delincuentes se ponen de acuerdo antes, luego cometen delitos en diferentes tiempos y lugares.

Por La Unidad del Acto y Pluralidad del Resultado: concurso ideal, concurso real. Concurso Ideal de Delitos (Delito Compuesto) Con una sola acción se violan varios bienes jurídicos. Ej. , una acción como una patada puede causar dos delitos: lesiones y atentado. Golpear a una mujer embarazada produce delitos como: lesiones y aborto. Se sanciona con pena del delito más grave, se puede aumentar hasta un máximo de una cuarta parte del delito más grave.

[7] **Jorge Machicado, Margot Mariaca , Ermo Quisbert, Clasificación del delito, 2007, www.enj.org**

Concurso Real de Delitos. Dos o más acciones u omisiones dan a lugar a dos o más delitos. Ej., Explosión de automóvil con bomba en centro comercial. Las acciones que generaron pueden ser: apoderamiento de un automóvil, instalación de la bomba. Los delitos son: robo de automóvil y terrorismo.

Por la Naturaleza Intrínseca: común, político, social, contra la humanidad

Delito común. Lesiona los intereses tutelados de los particulares, ej. , la vida, el patrimonio, la libertad.

Delito político. Criterios: Objetivo. El delito político es aquel que lesiona la organización política y social del estado.

Criterio subjetivo. Es aquél que lesiona la organización política y social con voluntad altruista y de sacrificio.

Criterio mixto. El delito político es aquél inspirado con fines generosos atenta contra la seguridad externa e interna de un Estado, persiguiendo mantener el orden establecido o cambiarlo a formas más superiores.

Delitos contra la Humanidad. Son los que atentan contra los derechos esenciales de la persona humana. Ej. , vida, nacionalidad, religión, opinión, etc.

La Convención Internacional sobre el Genocidio de 1948 cataloga como Delitos contra la Humanidad a los siguientes:

- El homicidio de grupo, [8]
- El exterminio. (Acabar del todo con la fuerza),
- La deportación en tiempo de paz,
- El genocidio,
- La reducción a la servidumbre,
- La persecución política o religiosa.

[8] **Jorge Machicado, Margot Mariaca , Ermo Quisbert, Clasificación del delito, 2007, www.enj.org**

Los delitos contra la humanidad se caracterizan por: Son cometidos debido a raza, nacionalidad o discrepancia política; y, Sé atentó contra la población civil; inclusive contra la propia población en los "golpes de Estado". [9]

2.1.2 Delito Informático

Las tecnologías de la información y comunicación están cambiando la sociedad en todas partes del mundo aumentando la productividad, acelerando el tiempo de respuesta, mejorando los procesos en las entidades, pero este desarrollo viene acompañado con nuevas formas de delincuencia informática.

"La delincuencia informática es difícil de comprender o conceptualizar plenamente. A menudo, se la considera una conducta proscrita por la legalización y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos." [10]

La Operación. El modus operandi de los delincuentes consiste en averiguar datos de clientes de bancos, verificar saldos de cuentas y realizar la transacción en minutos, en un solo tiempo, sacando para el efecto el dinero de la cuenta A, transfiriéndolo a la cuenta B, trasladándolo a la cuenta C y, finalmente, retirando el dinero por cajero automático.

Hacen que se les cuelgue o colapse la página web a los clientes del banco, quienes al verse fallida su transacción creen que se trata de un error de la computadora y entonces la apagan. Ese momento es aprovechado por los delincuentes informáticos para copiar claves de ingreso a las cuentas de sus víctimas y transferirse el dinero.

El cliente se da cuenta del atraco vía Internet cuando vuelven a conectarse a la página web del banco.

---

[9] **Jorge Machicado, Margot Mariaca , Ermo Quisbert, Clasificación del delito, 2007, www.enj.org**

[10] **Naciones Unidas , Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal – Delitos Informáticos, 25 de abril del 2005 , p. 1, www.unis.unvienna.org**

Delincuencia, a Tono con la Tecnología. "En el desarrollo de la tecnología, el problema radica en que la conducta humana parece ser que está inclinada al delito, a conseguir satisfacción a sus deseos a toda costa.

Señala que, con el desarrollo de la informática, aparece también lo que se denomina "delito informático".

De la misma forma que muchas personas se han dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras tratan de utilizar la tecnología, las computadoras y sistemas, para actividades ilícitas." [11]

"Delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin". [12]

2.1.2.1 Tipos de Delincuencia Informática

2.1.2.1.1 Los Virus Informáticos

Atacan a las propias tecnologías de la información y las comunicaciones, como los servidores y los sitios Web, causan considerables perjuicios a las redes comerciales y de consumidores.

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.[13]

Los virus, habitualmente, remplazan archivos ejecutables por otros infectados con código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que

[11] **Diario Hoy, Cinco delitos Informáticos cada día, 4 de Octubre del 2010, p.20**
[12] **María de Luz Lima, Revista Judicial, Derecho Ecuador, 2010, www.derechoecuador.com**
[13] **Fundación Wikimedia, Inc., Virus Informático, 8 de mayo del 2012, es.wikipedia.org**

solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

La manera de funcionar de un virus es la siguiente:

- Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario.

- El código del virus queda residente en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

- El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución.

- Se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa. [14]

2.1.2.1.2 El Vandalismo Electrónico y la Falsificación Profesional

No obstante los avances tecnológicos en materia de seguridad informática que las empresas han implantado para evitar las infiltraciones a sus sistemas computacionales y el robo de información, el descuido de los empleados sigue representando el factor primordial por el que los "vándalos informáticos" siguen teniendo éxito.

Estas debilidades son continuamente aprovechadas por los delincuentes dentro de lo

[14] **Fundación Wikimedia, Inc., Virus Informático, 8 de mayo del 2012, es.wikipedia.org**

que es la "ingeniería social", una habilidad utilizada en el mundo de la informática y por la que se manipula al personal de las empresas para así obtener información confidencial o simplemente provocar problemas.

Con la ingeniería social hay "miles" de maneras para perpetrar y robar información empresarial o personal; además, los ataques se pueden realizar con equipos que cuestan unos cuantos dólares. [15]

2.1.2.1.3 La Falsificación.

Es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos (bienes o servicios), con el de fin hacerlos parecer como verdaderos, o para alterar o simular la verdad.

Las falsificaciones pueden ser realizadas, entre otros, respecto a documentos públicos o privados, monedas, billetes u otros valores, arte y productos de marcas comerciales. En los primeros casos es un delito que afecta la fe pública, pudiendo llegar a ser una modalidad de fraude, mientras el último se entiende que es una vulnerabilidad de la propiedad industrial. [16]

2.1.2.1.4 El Robo o Fraude

Perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

2.1.2.1.5 Sabotaje Informático

Todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

---

[15] **Mundo Contact, Persiste el éxito del "vandalismo informático", 31 mayo 2010, www.mundocontact.com**

[16] **Fundación Wikimedia, Inc., Falsificación, 18 de mayo del 2012, es.wikipedia.org**

Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

- ***Conductas dirigidas a causar daños físicos:*** El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema.

- ***Conductas dirigidas a causar daños lógicos:*** El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático. [17]

2.1.2.1.6 Ingeniería Social

Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. [18]

[17] **Joaquin Galileo Soto Campos , Tipificación de los delitos informáticos – capitulo 9, 13 Septiembre del 2010, www.emagister.com**

[18] **Fundación Wikimedia, Inc., Ingeniería Social (Seguridad Informática), 10 de abril del 2012, es.wikipedia.org**

- **El phishing** o la inundación de mensajes supuestamente de origen conocido (spam spoofing) es la construcción de mensajes de correo electrónico con páginas Web correspondientes diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que anuncian como provenientes de bancos, subastas en línea u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.

  "**El Phishing** es clásico es el delito consistente en falsificar una página web que simula pertenecer a un Portal de Pagos o hasta de un Banco y al cual el usuario, previo mensaje de correo electrónico conminatorio es convencido a ingresar los datos de su tarjeta de crédito, con el propósito de una supuesta regularización, a causa de un supuesto error. Obviamente que esa tarjeta de crédito será utilizada para realizar compras ilegales a través de Internet.

Funcionamiento del Phishing

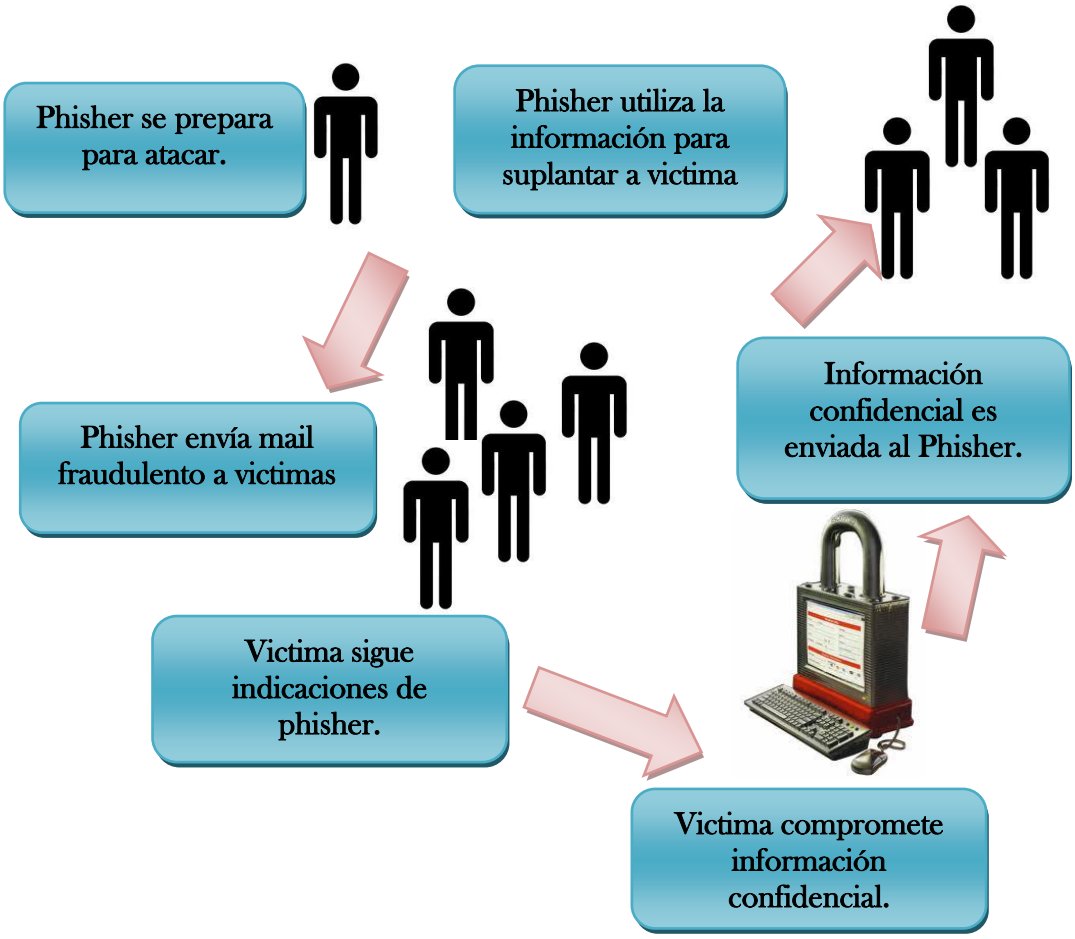


Figura 2.1 Funcionamiento del Phishing.

Fuente: Autores

Habitualmente los kits de creación de phishings que facilita la creación de páginas falsas de distintas entidades son contenidos en tres partes:

- La réplica de la página web que pretende ser simulada. Esta consta a su vez de páginas HTML, JavaScript, etc. que normalmente son colgadas en cualquier servidor y se debe incitar al usuario a visitarla. Es muy sencillo de obtener puesto que vale con "descargar" con algún programa la web legítima.

- La lógica del robo de contraseñas. Normalmente es un programa PHP que, o bien envía las contraseñas de formulario por correo electrónico, o bien las almacena en un archivo en el propio servidor y el atacante las obtendrá de ahí más adelante. Suelen ser apenas unas líneas de

código muy sencillas. En el kit, lo deja todo preparado para que el usuario solo deba modificar la dirección a la que quiere que vayan a parar las contraseñas robadas.

- Un correo que, con cualquier excusa, invita al usuario a visitar la web simulada. Suele contener un logotipo y será enviado de forma masiva a miles de cuentas de correo. Se suelen utilizar programas específicos para el envío masivo de correos o programas también en PHP que se aprovechan del motor de correo de páginas de terceros. Este kit recopila estos tres elementos para una buena cantidad de bancos y entidades de Internet: Desde Youtube, Gmail, o Facebook, hasta Banamex, Cajamadrid... pasando por eBay y MegaUpload.[19]

- **El Scamming** por el contrario, el la típico labor que conducen a una estafa. Por lo general empieza con una carta enviada en forma masiva con el nombre del destinatario, y al cual le pueden ofrecer una serie de oportunidades de ganar dinero, premios, préstamos a bajo interés, etc.

  - Oportunidad del cobro de una suma de dinero en algún país lejano como resultado de una resolución judicial.

  - Una persona "amiga" en el extranjero lo refirió para el sorteo de un viaje en crucero durante 7 días, para dos personas.

  - Préstamos de dinero o refinanciamiento de deudas a muy bajo interés.

  - Comunicación de haber ganado un premio en una Lotería.

  - Apelar al dolor humano para contribuir a una causa noble. Puede estar combinado con el Phishing.

[19] **Sergio de los Santos - Hispasec Sistemas, Kit de creación de phishing "especial", 3 de Febrero del 2011, www.hispasec.com**

- Venta de software por Internet, supuestamente legal y licenciado. [20]

- **El Pharming** método utilizado para enviar a la victima a una página web que no es la original solicitada.

- **El Skimming** robo de la información que contiene una tarjeta de crédito.

- **Sniffing** la habilidad de un agresor de escuchar a escondidas las comunicaciones entre hosts de la red.

Figura 2.2 Legislación - Ecuador

Fuente: Autores

[20] **Carlos Cabezas López, Delitos Informáticos, 2010, www.drechoinformatico.galeon.com**

INFRACCIONES INFORMÁTICAS	REPRESIÓN	MULTAS
Delitos contra la información protegida (CPP Art. 202) 1. Violentando claves o sistemas 2. Seg. nacional o secretos comerciales o industriales 3. Divulgación o utilización fraudulenta 4. Divulgación o utilización fraudulenta por custodios 5. Obtención y uso no autorizado	 6 m. - 1 año 3 años 3 a 6 años 9 años 2 m. - 2 años	 $500 a $1000 $1.000 - $1500 $2.000 - $10.000 $2.000 - $10.000 $1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	6 años	---
Falsificación electrónica (CPP Art. 353)	6 años	---
Daños informáticos (CPP Art. 415) 1. Daño dolosamente 2. Serv. público o vinculado con la defensa nacional 3. No delito mayor	6 m. - 3 años 5 años 8 m. - 4 años	$60 – $150 $200 - $600 $200 - $60
Apropiación ilícita (CPP Art. 553) 1. Uso fraudulento 2. Uso de medios (claves, tarjetas magnéticas, etc.)	 6 m. - 5 años 5 años	 $500 - $1000 $1.000 - $2.00
Estafa (CPP Art. 563)	5 años	$500 - 1.000

Tabla 2.1 Infracciones informáticas (CPP)

Fuente: Autores

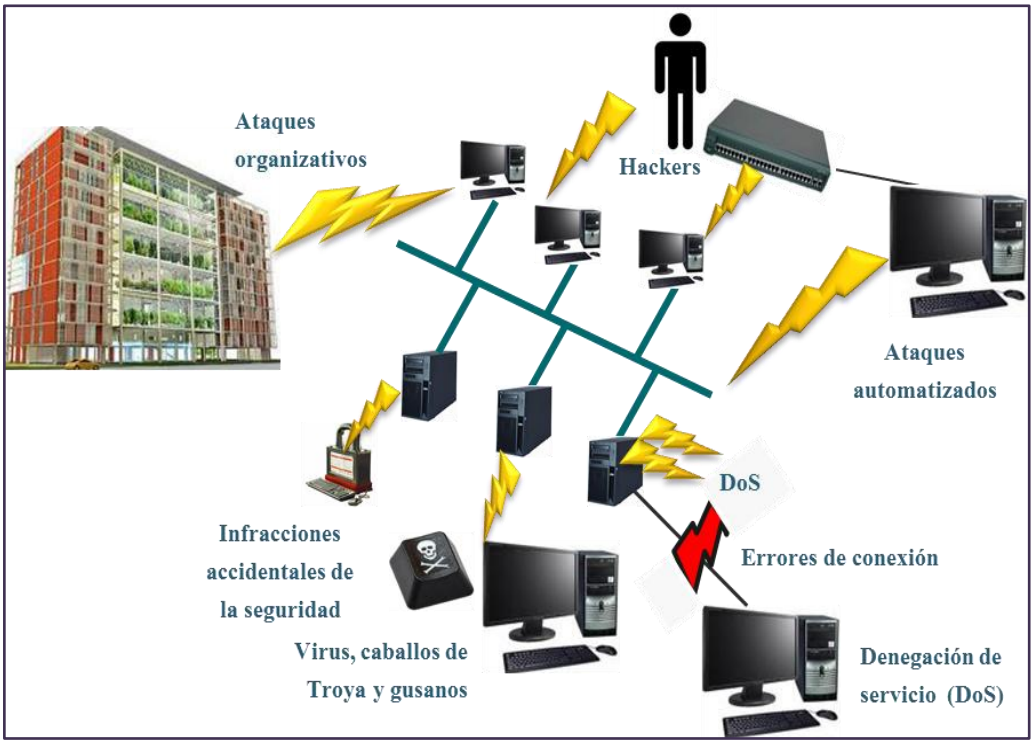


Figura 2.3 Tipos de ataques más comunes

Fuente: Autores

2.1.2.2 Software Utilizados por Atacantes

Spyware.- Recolecta y envía información privada sin el consentimiento y/o conocimiento del usuario.

Dialer.- Realiza una llamada a través de modem o RDSI para conectar a Internet utilizando números de tarificación adicional sin conocimiento del usuario.

Keylogger.- Captura las teclas pulsadas por el usuario, permitiendo obtener datos sensibles como contraseñas.

Adware.- Muestra anuncios o abre páginas webs no solicitadas.

Backdoor.- O puerta trasera, permite acceso y control remoto del sistema sin una autentificación legítima.[21]

[21] **Sonia Córdova, José Hinca, otros, Robos y Fraudes Informáticos, 17 Noviembre del 2008, www.slideshare.net**

2.1.2.3 Tipos de Delitos Informáticos

2.1.2.3.1 Clasificación según el "Convenio sobre la Ciberdelincuencia" de 1 de Noviembre de 2001

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". En este convenio de propone una clasificación de los delitos informáticos en cuatro grupos:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**

    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la comisión de delitos.

    Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.[22]

- **Delitos informáticos:**

    - Falsificación informática mediante la introducción, borrada o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

[22] **Departamento de Peritaje Informática - Computer Forensic, Tipos De Delitos Informáticos, 2012, delitosinformaticos.info**

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

- **Delitos relacionados con el contenido:**

    - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**

    - Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.

- Insultos o amenazas con motivación racista o xenófoba.

- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad. [23]

[23] **Departamento de Peritaje Informática - Computer Forensic, Tipos De Delitos Informáticos, 2012, delitosinformaticos.info**

2.1.2.3.2 Clasificación según la página de la Brigada de Investigación Tecnológica de la Policía Nacional Española

- **Ataques que se producen contra el derecho a la intimidad:**

  Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal).

- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:**

  Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal).

- **Falsedades:**

  Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal).

- **Sabotajes informáticos:**

  Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal).

- **Fraudes informáticos:**

  Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal).

- **Amenazas:**

  Realizadas por cualquier medio de comunicación. (Artículos 169 y ss.del Código Penal).

- **Calumnias e injurias:**

  Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal).

- **Pornografía infantil:**

  Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos. La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187).

  La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189).

  El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (art 189). La posesión de dicho material para la realización de dichas conductas. (art 189)[24].

[24] **Departamento de Peritaje Informática - Computer Forensic, Tipos De Delitos Informáticos, 2012, delitosinformaticos.info**

2.1.2.4 Las TICs

Las tecnologías de la información y la comunicación es el conjunto de recursos, herramientas, técnicas que procesan, almacenan, administran, y transmiten la información representada en varias formas, que facilitan el aprendizaje, desarrollo de habilidades, disminución de tiempo y respuestas.

Incluyen en las TICs la informática, tecnologías, telemática, multimedia, medios de comunicación de todo tipo como la social, interpersonales tradicionales con soporte tecnológico.

Las tecnologías de la información y la comunicación ha mejorado la vida de todas las personas, empresas, entidades por que la información se la puede obtener en muchos sitios, antes reposaba solo en libros o conocimientos humanos, en la actualidad con el internet el acceso a la información requerida se ha logrado con rapidez, también el contacto entre personas para comunicarse y realizar negocios; no es necesario movilizarse de un lugar a otro para realizar transacciones o concluir negocios solo lo hacemos con un clic.

Las opiniones pueden ser vistas por todos y a su vez son disputadas entre sí, o bien para la elección o modificación de algún tema o articulo por medio de los blogs.

La interactividad y la interconexión hoy en día son instantáneas, con una calidad elevada de imágenes y sonidos.

En la educación se ha desarrollada varias formas de aprender más interactivas con nuevos estilos y ritmos de aprendizajes, las herramientas y materiales que contienen las TICs facilitan la comprensión para los estudiantes de todos los niveles e instituciones.

Se ha elevado la compra de infraestructura informática, de centros de estudio computacional, instituciones comunitarias, capacitaciones a docentes para la elaboración de paquetes en base a las TICs para un desarrollo sostenible del país.

Se incorporo la educación a distancia a partir de los años 60, principalmente para adultos, actualización profesional, trabajadores de tiempo completo, para aportar el progreso socioeconómico propio y del país.

Continuando con los avances científicos y en la globalización económica, social y cultural, las TIC contribuyen a la obsolescencia de los conocimientos causando varias cambios y transformaciones en las estructuras sociales, culturales y económicas, el impacto positivo de las TIC en la actualidad hace cada vez más complicado el no prescindir de ellas.

Sus principales aportaciones a las actividades humanas es la disminución del trabajo cotidiano pero siempre necesitan de cierta información para realizarlo, los procesamientos de datos y cierta comunicación entre personas, las TIC nos ayudan con todos estos aspectos.

2.1.2.4.1 Características de las TICs

- **Inmaterialidad**

  Las tecnologías de la información y la comunicación convierten la información en inmaterial a un medio físico por medio de la digitalización en dispositivos físicos de pequeños tamaños como en discos duros, flash memory, CDs y esta información es visualizada en cualquier lugar, en cualquier momento o compartida por medios de redes de comunicación de manera transparente e inmaterial.

- **Instantaneidad**

  La información que se va a transmitir es de forma instantánea sin importar la ubicación física y a esto se lo denomina "autopistas de la información".

  El espacio no real es definido como espacio virtual donde se guarda la información y puede ser utilizado inmediatamente e inmaterialmente, sirve como un almacenamiento de cualquier tipo de información.

- **Aplicaciones Multimedia**

  Mediante las TICs tenemos aplicaciones multimedia que son muy amigables para los usuarios y hace que la interactividad con el medio tecnológico se mejor, su sencilla comunicación y respuesta hace el ahorro de tiempo.

  Permite una conexión bidireccional, puede ser sincrónica o asincrónica, de persona a otra persona o a un grupo para comunicarse según sus intereses.

  La comunicación no solo será por medio de texto sino también mediante imágenes, sonidos, animaciones, tablas, etc., en un mismo documento integran informaciones multi-sensoriales, desde un modelo interactivo.

2.1.2.4.2 Conductas Delictivas con uso de las TICs en Ecuador que Gestiona la Administración de Justicia

Las conductas delictivas que se cometen con más frecuencia a través de Internet tienen que ver sobre todo con los siguientes aspectos:[25]

- Menores,
- Amenazas, calumnias e injurias,
- Estafas a través del comercio electrónico,
- Vulneración de derechos de propiedad intelectual e industrial,
- Accesos a datos reservados de carácter personal,
- Acceso a secretos de empresa,
- Daños en sistemas informáticos,
- Venta de productos prohibidos a través de Internet,
- La apología del terrorismo y la xenofobia.

[25] **Plan Operativo Unidad de Delitos Informático, 2010 , Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito**

2.1.2.5 Conductas Delictivas más Comunes

- El ciudadano compartió su vida y su intimidad con alguien que en ese momento le hizo **fotos íntimas**. Ahora las ha **publicado en Internet** o se las envía a familiares o a cualquier persona con un ánimo claro de atentar contra su dignidad, menoscabando su fama o su imagen. Se tipificaría como **delito de injurias.**

Si se ha hecho un **montaje fotográfico** de imágenes en las que se encuentra un ciudadano, su cara o algún rasgo que por el cual se le pueda:

- Identificar, y ese montaje se ha **difundido** a través del correo electrónico o se ha publicado en Internet. Se tipificaría como **delito de injurias**. Si además el correo electrónico corresponde a una empresa, se puede pedir también la responsabilidad a la empresa.

- Si se está recibiendo llamadas telefónicas o recibe contactos de personas que le solicitan **favores o servicios sexuales**, sin que haya ofrecido esos servicios, quiere decir que sus datos personales se han publicado en Internet, en algún Sitio Web que se anuncian personas para mantener relaciones o páginas de contactos. Se tipificaría como **delito de injurias**[26]

- Si se ha **insultado** a través de cualquier tipo de foros de debate o Chat, correo electrónico o en un Sitio Web, mediante expresiones que claramente lesionan la dignidad y estimación o menoscaba su fama. Se tipificaría como **delito de injurias.**

- Si por cualquier contenido que se ha difundido en Internet, a través de la publicación del mismo en una página Web, o su comunicación a través del correo electrónico, foros, Chat o cualquier otro medio, **se acusa** de haber **cometido un delito** que en realizad no ha cometido, Se tipificaría como delito de Injurias calumniosas.

[26] **Plan Operativo Unidad de Delitos Informático, 2010 , Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito**

- Si se ha recibido a través de Internet, o se ha encontrado en un medio de Internet que se haya consultado, amenazas dirigidas a la persona, por las cuales se deduce un daño o perjuicio a su persona, y se le exige o no contraprestación de cualquier naturaleza. Se tipificaría como **delito de amenazas.**

- Si se ha efectuado la **compra de un producto** determinado o la contratación de un servicio a través de **comercio electrónico**, efectuó el pago a través de transferencia bancaria o tarjeta de crédito, y después del plazo de entrega **no se ha recibido el producto o se ha recibido otro de interiores características o calidades**, Se tipificaría como **delito de estafa**. Por otra parte, se puede revisar el sitio Web a través del cual se ha realizado la estafa y comprobar si cumple con las exigencias de la normativa de comercio electrónico.

- Si un ciudadano forma parte de una empresa u organización que realiza comercio electrónico, y después de haber entregado el producto y haber cobrado el importe del mismo, el banco o la institución financiera se pone en contacto con el ciudadano y **le retira el abono**, porque el titular de la tarjeta ha rechazado los cargos. Se tipificaría como **delito de estafa.**

- Una práctica habitual de fraude en el comercio electrónico es la utilización de **tarjetas ajenas**. Si se ha visto en el extracto de la tarjeta el importe de un cargo por una compra de comercio electrónico que no se haya realizado, otra persona la ha realizado con los datos de su tarjeta. Se tipificaría como **delito de estafa.**

- Existen sitios Web de contenidos para adultos que después de una primera visita en la que se puede ver la completa oferta de servicios de la página como fotos, vídeos, Chat, contactos, etc. ofrecen contenidos que aparentemente son gratuitos, pero a través de una letra pequeña o sin avisar al respecto, con solo pulsar en ENTRAR o ACEPTAR, se está accediendo a través de programas. Se tipificaría como **delito de estafa**.

- Internet se ha convertido también en un foro donde los tipos más sorprendentes de **timos** se pueden llegar a dar. Se suele hablar de **ofertas millonarias**, o multimillonarios que quieren compartir su fortuna o simplemente fondos de inversión o de pensiones que no existen. Además prometen que por irrisorias inversiones iniciales se pueden llegar a alcanzar fortunas inigualables. Se tipificaría como **delito de estafa**.

- Si un ciudadano se da cuenta de que **su ordenador está siendo controlado** por cualquier otra persona desde Internet, sin su intervención, de tal suerte que se abren o cierran aplicaciones, se dan procesos que no se han activado o recibe mensajes extraños, puede que tenga defectos de seguridad o que a través de la conexión a Internet alguien haya logrado entrar en su sistema. Se tipificaría como **delito de descubrimiento y revelación de secretos**. Si por los mismos medios, tiene conocimiento de que un tercero ha tenido acceso o conoce información de carácter personal que se hallaba almacenada en su sistema y que no puede haber sido difundida por otra persona. Se tipificaría como **delito de descubrimiento y revelación de secretos**.

- Si un tercero está utilizando sus **nombres de usuario y contraseña o cualquier otra información**, este tercero ha usurpado su identidad, y lo puede haber hecho a través de un acceso remoto (PHISHING) o de programas troyanos que le han permitido acceder a su ordenador. Se tipificaría como **delito de estafa**, un **delito de descubrimiento y revelación de secretos y de un delito de usurpación del Estado civil**.

- Si sus sistemas informáticos han sido **infectados por un virus**, con independencia de que disponga o no de antivirus, y debe de formatearse el sistema y volver a instalar todos los programas, Se tipificaría como **delito de daños en sistema informático**. Se ubica el mismo delito si alguien accede a su sistema y le borra datos o ficheros.

- Si alguien está utilizando su ordenador o el de su empresa para dar algún tipo de **servicio en Internet** porque los programas van más despacio y siente que

su sistema se ha vulnerado. Se tipificaría como **delito de defraudación en el fluido de las telecomunicaciones.**

- Si se tiene constancia que cualquier **dato o información relevante para su empresa**, como proyectos, cartera de clientes, datos personales de empleados o personal, datos económicos, modos de trabajo u otros datos reservados, **son manejados por terceros** que pretenden una competencia desleal o el descrédito y el perjuicio de la empresa y de su personal, y esa información se conserva en sistemas informáticos. Se tipificaría como **delito de descubrimiento y revelación de secretos de empresa**, además de poder actuar valorando las infracciones en materia de protección de datos o propiedad intelectual e industrial, según los contenidos accedidos.

- Si un ciudadano es **autor de un programa de ordenador, base de datos o aplicación informática**, lo tiene debidamente registrado, y ha comprobado que se está comercializando, distribuyendo o intercambiando por Internet sin su consentimiento. Se tipificaría como **delito contra los derechos de propiedad intelectual**.

- Si un ciudadano es **autor de música, películas, vídeos, programas de ordenador, o de cualquier obra literaria, científica o artística** y ha tenido conocimiento de que la misma se está divulgando, comercializando o intercambiando a través de Internet, por un tercero, empresa, organización o persona que no tiene su consentimiento ni siquiera posee los derechos de explotación de la obra. Se tipificaría como **delito contra la propiedad intelectual**.

- Si un ciudadano posee **productos o signos distintivos patentados o registrados** por él o su empresa, y tiene conocimiento que se están utilizando o comercializando a través de Internet. Se tipificaría como **delito contra los derechos de propiedad industrial**.

- Si se tiene conocimiento de un sitio Web donde **ofrecen o se comercializan imágenes de pornografía infantil, contenidos que incitan al terrorismo, a la violencia o al odio racial**, conoce la dirección donde los contenidos se ofrecen. Se tipificaría como **delito de pornografía infantil u otros**.

- Si se ha conocido que un menor ha recibido un mensaje con contenidos pornográficos, puede tratarse de un **delito de provocación sexual**. Si se tiene conocimiento de que un menor ha recibido proposiciones de contactos sexuales a través de Internet o le han solicitado fotografías. Se tipificaría como **delito de corrupción de menores**.

2.1.2.6 El Especialista en la Administración de Justicia en la Sociedad Ecuatoriana (PERITO)

La conceptualización que brinda Juan Carlos Riofrío, es que "los peritos en general, para la administración de justicia, son personas expertas en una materia, capaces de aportar al juez conocimientos que no posee, con el fin se servir de lentes de aumento para la justicia con el fin de aclarar el asunto litigiosos en revisión.", entonces, bajo esta conceptualización, el perito es un auxiliar de la justicia, que no persigue como objetivo resolver un problema operativo, sino revelar y/o explicar la causa y el porqué de dichos problemas, luego de un análisis y profundo estudio.

Emilio del Peso Navarro, aporta una definición para el perito informático en la cual lo describe como "un perito especializado en el área de las tecnologías de la información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis. Así puede influir para su selección la plataforma tecnológica el lenguaje de programación usado, el sistema de base de datos, sistemas operacional, entre otros.", entonces, tomando en consideración esta descripción, al ser el perito informático un profesional que va a emitir un criterio u opinión, la cual, debe estar fuertemente sustentada tanto en la parte técnica como científica, logre llegar a conclusiones objetivas e imparciales sobre un hecho, y no solo basarse en impresiones u opiniones.

De acuerdo a lo contemplado en nuestra legislación en el Art. 94 del Código de

Procedimiento Penal (CPP), "son peritos los profesionales especializados en diferentes materias que hayan sido acreditados como tales, previo proceso de calificación del Ministerio Público".

En el caso de que no se encuentren peritos habilitados en la rama a investigar el mismos CPP en su Art. 95 establece que "si en el lugar donde se deba realizar la diligencia no hubiera peritos habilitados, el Fiscal nombrará a personas mayores de edad, de reconocida honradez y probidad, que tengan conocimientos en la materia sobre la que deban informar", conviene entonces que las personas designadas en calidad de perito, para estos casos, deban acreditar el conocimiento suficiente y verificable en la materia, sobre la cual van a emitir un criterio u opinión.

El Ministerio Público del Ecuador, mantiene el registro de los peritos acreditados a nivel nacional en el cual existen alrededor de 1433 peritos acreditados en diferentes ramas como: la medicina, química, criminalística, documentología, traducciones, financieros, contables, avalúos, entre otras, incluidos peritos en la rama de informática y telecomunicaciones.[27]

2.1.2.7 Perfil del Especialista Informático en la Administración de Justicia en la Sociedad Ecuatoriana en TICs

De acuerdo a Jeimy Cano, un perito informático (Especialista en la Administración de Justicia TICs), requiere de una formación exigente y detallada no solo en la materia en la que se requiere de su conocimiento sino también de procedimientos legales, legislación nacional e internacional, fundamentos de criminalística y psicología que le permitan un conocimiento más profundo de los casos analizados, ya que como perito es un garante de la verdad en un proceso. Por lo expuesto, es clave que el perito acredite experiencia, conocimientos teóricos y prácticos, habilidades en la aplicación de procedimientos y metodologías, y que sus informes sean metódicos y estructurales, entre otros. El perfil del perito informático debe cumplir con algunas de las funciones que se destacan a continuación:

- Identificación y recolección de evidencias en medios magnéticos.

[27] **Plan Operativo Unidad de Delitos Informático, 2010 , Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito**

- Comprensión y práctica en procedimientos de revisión y análisis forenses.

- Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática.

- Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.

- Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación informática.

- Comprensión de los diferentes sistemas de archivos asociados con sistemas operativos, acceso a archivos temporales, de cache, de correo electrónico, de Web, etc.

- Conducir de manera detallada, recuperación de datos de todas las porciones de un disco.

- Comprensión de aspectos de Internet.

- Comprensión de técnicas de rompimiento de contraseñas y claves de seguridad.

- Comprensión general de los temas relacionados con investigaciones forenses.

Las investigaciones forenses aplicables a la informática, requieren de profesionales con altos conocimientos en tecnologías de la información, que se ajusten a la aplicación de procedimientos científicamente probados válidos y reconocidos sobre las evidencias que vulneran o comprometen sistemas de tipo informático, para ellos existen certificaciones u avales profesionales, que pueden ser obtenidos por los profesionales en las ramas de informática.

A fin de desarrollar el perfil forense o de seguridad requerido en las ramas de informática, existen instituciones internacionales tales como IACIS (International

Association of Computer Investigative Specialist), HTCN (High Technology Crime Network), ACFE (Association of Certified Fraud Examiners), EC – Council, que en este sentido han desarrollado programas de certificación aplicables a la informática, que permiten luego de seguir un programa de especialización desarrollar habilidades y capacidades deseables en los especialistas informáticos ante la investigación de un hecho, la siguiente tabla muestra por ejemplo algunas certificaciones de este nivel:

Es menester recalcar, que el perito debe contar, además de sus vastos conocimientos, con altos valores éticos morales y profesional (teoría del deber y/o deontológica), que acredite la seriedad de su diligencia ante un proceso legal en que se hayan requerido sus conocimientos y habilidades para la investigación de un acto ilícito que se haya cometido.

Después de que se ha realizado el proceso de investigación por parte del perito, y luego de haber entregado su informe, él podría ser llamado por la autoridad competente, para aclarar u ampliar su informe, ya sea de manera escrita u oralmente mediante declaraciones durante un proceso de indagación acusación, penal, por ello, debe tener la capacidad de comunicar lo que ha realizado y estudiado dentro de su análisis pericial, debe justificar al juez, fiscal, o tribunal, porque se le debe creer en lo que respecta a sus conclusiones, las herramientas o técnicas que ha utilizado durante el proceso de análisis e incluso, podría indagarse sobre los procedimientos realizados y las técnicas utilizadas durante su investigación.

2.1.2.8 Perfil del Delincuente Informático

A partir del año 2000, el uso extendido y generalizado de internet, pone al alcance a muchos delincuentes y oportunistas una plataforma para conseguir dinero de manera rápida y relativamente anónima. Durante los tres o cuatro años siguientes, los esquemas y recursos utilizados para realizar fraude evolucionan de manera sorprendente, del mismo modo que la proliferación de nuevas comunidades y asociaciones orientadas a realizar fraude.

Aproximadamente a partir del año 2004, en cuanto estas carencias en cuanto a organización, estructura y calidad se empezaron a solventar, el escenario empezó a ser realmente peligroso.

En este punto, incluso los estafadores solitarios, que siempre los ha habido y siempre los habrá, interactúan con otros individuos en comunidades orientadas única y exclusivamente a realizar fraude. El hecho de poder encontrar cualquier recurso o asociación que se necesite online, potencia la creación de nuevas asociaciones de mayor magnitud potencial.

Se empiezan a utilizar esquemas de fraude mucho más agresivos, los ataques ya no solo se basan en la ingenuidad o ignorancia de las víctimas. Se llevan a cabo delitos de extorsión mediante ataques de denegación de servicio, infección con malware que pide rescate económico para recuperar el sistema, código que atemoriza al usuario sobre el contenido ilegal de su PC, etc. Las herramientas utilizadas sufren una sofisticación muy significativa, del mismo modo que los ataques en las que son empleadas.

Las víctimas son principalmente usuarios domésticos, aunque además de realizar ataques indiscriminados también se detectan ataques muy dirigidos a individuos de perfiles más apetitosos para los estafadores (ejecutivos, altos cargos, directivos, etc.).Nadie parece estar a salvo.

Las personas autoras de delitos informáticos poseen características muy diversas.

Aquella persona que "entra" ilegítimamente y en forma remota en un sistema informático sin intenciones delictivas, es muy diferente, por ejemplo, del empleado de una institución financiera que, en forma fraudulenta, desvía fondos de las cuentas de sus clientes. En relación a las características personales de aquellos que cometen delitos en Alta Tecnología, debe tenerse presente que generalmente lo siguiente:

En general son personas que no poseen antecedentes delictivos.

- La mayoría de sexo masculino.

- Actúan en forma individual.

- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación “hackers”.

- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.

- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

- En el caso de los “hackers”, realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovecha la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).

- Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia los han catalogado como “delitos de cuello blanco”, (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico). Este término fue introducido por primera vez por el Criminólogo norteamericano Edwin SUTHERLAND, en el año 1943.

Asimismo, este conocido criminólogo señala un sinnúmero de conductas que no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, entre otros.

2.1.2.9 Delincuencia y Criminalidad Informática en la Sociedad

Carlos Sarzana, describe en su obra "Criminalitá e Tecnología", que los crimines por computadora comprenden "cualquier comportamiento criminógeno, en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como un simple símbolo", entonces según esta descripción las personas que cometen delitos o crímenes informáticos, están enmarcadas dentro de lo que se conoce como criminología, y la investigación de dichos delitos, están sujetos a las ciencias de la criminalística.

Es preciso que se reconozca la diferencia entre la criminología y la criminalística; La criminología trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística según Montiel Sosa , se definen como "una ciencia multidisciplinaria que reúne conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen" , la criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, y se apoya de métodos y técnicas propias del trabajo de las diferentes disciplinas.

Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos informáticos, ya que han tenido un repunte a los largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

2.1.2.10 Medios de Prueba de las Obligaciones Reconocidos en la Legislación Civil Ecuatoriana.

Tanto en la prueba de las obligaciones en materia civil, como en el resto de las áreas jurídicas, es posible adquirir elementos de convicción para convencerse de la verdad o falsedad de un hecho de tres maneras:

- La primera mediante una constatación de los hechos por medio de la observación personal del lugar en donde han sucedido, lo que jurídicamente se conoce con el nombre de inspección judicial.

- La segunda mediante el raciocinio que permite deducir el hecho desconocido en base a los hechos conocidos y probados en juicio, este medio de prueba se denomina presunciones,

- Y finalmente por las declaraciones de las partes o de terceros que pueden ser verbales o escritas, encontrándonos de este modo con la presencia de los documentos, testigos, confesión de parte, juramento deferido e informe de peritos.

Los medio de prueba deben ser expresamente reconocidos por la ley para ser admitidos en un proceso y necesariamente hay que acudir al derecho positivo para la determinación de los mismos. En el Art. 1715 del Código Civil Ecuatoriano es donde se encuentra determinado cada uno de los medios de prueba que se reconocen como tales por la legislación Civil Ecuatoriana en la pruebas de las obligaciones:

"Art. 1715 Incumbe probar las obligaciones o su extinción al que alega aquellas o esta. Las pruebas consisten en instrumentos públicos o privados, testigos, presunciones, confesión de parte, juramento deferido, inspección personal del juez y dictamen de peritos o de intérprete."

2.1.2.11 Evidencia Electrónica

A diferencia de otro tipo de pruebas, como puede ser la documentación en papel, las evidencias electrónicas son pruebas físicas aunque de carácter intangible, ya que generalmente son rastros registrados en equipos informáticos.

El ordenador registra los datos de todas las actividades que realiza. Dichos registros o logs son fundamentales en las investigaciones informáticas, siempre que se pueda comprobar que no han sido manipulados. Los servidores de correo, cortafuegos o el router también generan logs.

En ocasiones, para la adquisición o recolección de la evidencia electrónica, el perito informático utiliza herramientas especializadas en la investigación informática.

Durante la investigación, el perito informático se puede encontrar con algunos obstáculos, como por ejemplo la dificultad a la hora de reconstruir la evidencia electrónica debido a que los datos están dañados o han sido eliminados.

Al adquirir y tratar la evidencia electrónica, los elementos que deben regir el trabajo del perito informático son: la no alteración de la prueba y el principio de imparcialidad. En este sentido y con el fin de garantizar la autenticidad y seguridad de la información que constituye la prueba, la IOCE (International Organization on Computer Evidence) propone cinco principios sobre la adquisición y el tratamiento de la evidencia electrónica:

- Las acciones llevadas a cabo para adquirir la evidencia electrónica no deben modificarla.

- Las personas que accedan a la evidencia electrónica original deben estar formadas especialmente para ello.

- Toda aquella actividad referente a la adquisición, acceso, almacenamiento o transferencia de la evidencia electrónica, debe ser totalmente documentada, almacenada y debe estar disponible para revisión.

- Un individuo es responsable de todas las acciones llevadas a cabo con respecto a la evidencia electrónica mientras este en su posesión.

- Cualquier organismo que sea responsable de la adquisición, acceso, almacenamiento o transferencia de la evidencia electrónica debe cumplir estos principios.

2.1.2.12 Cadena de Custodia

La cadena de custodia es el procedimiento de control que se emplea para los indicios materiales afines al delito, desde su ubicación, hasta que son valorados por los diferentes funcionarios encargados de administrar justicia, y que tiene como finalidad no viciar el manejo que de ellos se haga, y así evitar la contaminación, alteración, daños, remplazos, contaminación o destrucción. Desde la ubicación, fijación, recolección, embalaje y traslado de la evidencia en la escena del siniestro, hasta la presentación al debate, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena, es la misma que se está presentando ante el tribunal, o el respectivo dictamen pericial.

Al recolectar las pruebas, lo importante es el significado, el valor que va a tener en el proceso de investigación y por medio de la cadena de custodia, este valor va a ser relevante, debido a que no se va a poder impugnar, al haberse acatado el procedimiento.

2.1.2.13 La Informática Forense (Herramienta del Especialista en Conductas Delictivas con uso de las TICS)

El FBI, conceptualiza la informática forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional. Este mismo organismo ha desarrollado programas que permiten examinar evidencia computacional.

Gerberth Adín Ramírez, identifica los objetivos de la informática forense con el fin de: perseguir y procesar judicialmente a los criminales; crear y aplicar políticas para

prevenir posibles ataques y de existir antecedentes evitar casos similares; compensar daños causados por los criminales o intrusos.

Esta ciencia relativamente nueva se aplica tanto para las investigaciones de delitos tradicionales tales como: fraudes financieros, narcotráfico, terrorismo, etc.; como para aquellos que están estrechamente relacionas con las tecnologías de la información y las comunicaciones, entre los que se tienen la piratería de software, distribución pornográfica infantil, tráfico de bases de datos, etc.

Adicionalmente, el desarrollo de la ciencia de la informática forense, es una técnica utilizada por los especialistas durante el proceso de investigación de los llamados delitos informáticos.

El análisis forense digital, según Miguel López Delgado, en un sentido formal es definido como "el conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que en determinado caso pueden ser aceptadas legalmente en un proceso judicial". Para esta ciencia se han identificado las fases que se consideran de relativa importancia ante un proceso de análisis forense[28]:

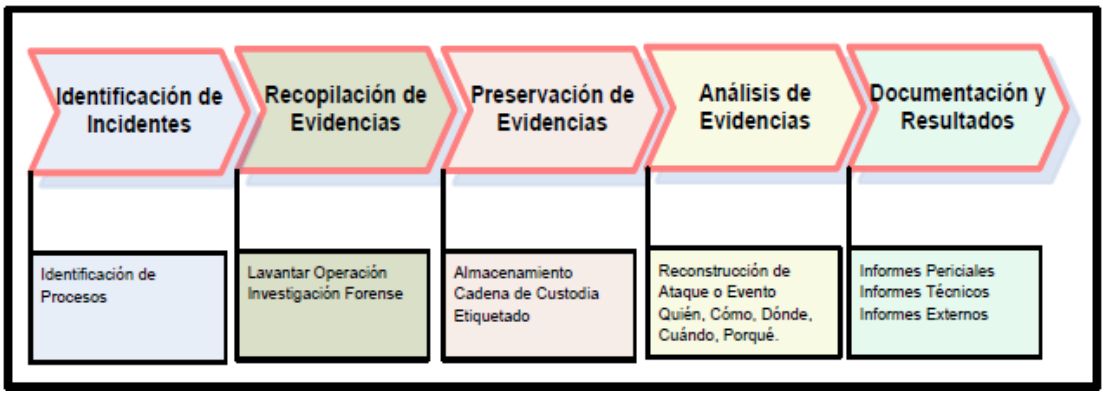


Figura 2.4 Fases de Análisis Forense Digital

Fuente: FBI

[28] **FBI, Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence, 1995, http://www.fbi.gov/**

2.1.2.14 Condiciones Legales Establecidas en la Legislación Ecuatoriana.

Antes de conocer las regulaciones que se han establecido en el Administración de Justicia en la Sociedad Ecuatoriana y que están relacionadas con las tecnologías de la información, se mostrará cual es la estructura general de dichas regulaciones, para ello, se toma como referencia la Pirámide Kelseniana. El cual es un recurso que permite ilustrar, la jerarquía de las normas jurídicas:[29]

Figura 2.5 Jerarquía de Leyes

Fuente: Internet

Desde los años ochenta, las Naciones Unidas han venido promoviendo por medio de la Uncitral (CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) una adecuación de las diferentes legislaciones mundiales a sus leyes modelos, entre los documentos aprobados por dicha comisión están, por ejemplo: la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas.

En Sudamérica, el primer país que se preocupó por estos temas fue Colombia, ya que en 1999 publica su ley 527, la misma que regula el comercio electrónico, firmas digitales y las entidades de certificación, luego en el mes de mayo del año 2000 Perú publica la ley 27269, sobre Ley de Firmas y Certificados Digitales. Luego, le siguen

[29] **Hans Kelsen, General Theory of Law and State, Harvard University, Editorial Porruo 1945**

en el 2001 Argentina y Venezuela en el año 2001, luego Chile y Ecuador en el año 2002.

Gerberth Adín Ramírez Rivera, expresa "para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes".

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

1) Ley Orgánica de Transparencia y Acceso a la Información Pública.

2) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3) Ley de Propiedad Intelectual.

4) Ley Especial de Telecomunicaciones.

2.1.2.15 Realidad Social de la Administración de Justicia frente a la Delincuencia con uso de las TICS

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros.

También se conformo comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presento en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la *criminalidad informática*.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución Política de la República, al hablar del Ministerio Público, señala que: "**El Ministerio Público prevendrá en el conocimiento de las causas**, **dirigirá y promoverá la investigación pre-procesal y procesal penal**. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "**el ejercicio de la acción pública corresponde exclusivamente al fiscal**". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto preprocesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a

perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el COMPUTER CRIME UNIT, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos. La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos,

las empresas y los individuos a estos peligros. Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones.

2.1.2.16 Limitaciones Tecnológicas en la Administración de Justicia

La distribución de las tecnologías de la información y las comunicaciones en todo el mundo no es uniforme. Existen vastas diferencias en los tipos y números de adelantos tecnológicos en diferentes partes del mundo. La denominada brecha digital fue reconocida en la Declaración del Milenio de las Naciones Unidas del 2000. [30]

La Declaración de Principios adoptada por la Cumbre Mundial sobre la Sociedad de la Información, establece que los beneficios de la revolución de la tecnología y la información están actualmente distribuida de manera desigual entre los países desarrollados y en desarrollo y dentro de las sociedades. Esta declaración también incluye el compromiso de transformar esta brecha digital en una oportunidad digital para todos en particular para aquellos que corren el riesgo de quedar rezagados y marginados.

Considerando este aspecto, no es inverosímil entonces, que el Departamento de Criminalística de la Policía Judicial, según consta en el listado que mantiene el Ministerio Público de los peritos, cuente solamente con un perito especializado en la rama de informática, aspecto que contribuye a que se contraten por necesidad a los profesionales acreditados o no, y que en muchas ocasiones estos no cuenten con la

[30] **Plan Operativo Unidad de Delitos Informático, 2010 , Unidad de Delitos Informáticos Fiscalía General del Estado, Sede Quito**

experiencia, los medios u herramientas y la formación adecuada para la ejecución de la investigación del acto ilícito. Si bien es cierto el Departamento de Criminalística, cuenta con la Sección de Análisis Informático y Telecomunicaciones y se ha determinado sus responsabilidades preliminarmente, tal como, consta en el Reglamento de la Policía Judicial, esta sección no se ha desarrollado, a favor de la sociedad ya sea por la falta de recursos o la falta de proyectos que contemplen iniciativas innovadoras que permitan el tratamiento de los delitos informáticos desde una perspectiva integral.

En este punto es prescindible destacar, que en Ecuador desde Abril del 2008 se encuentra habilitado el proyecto "Libertador", con el que se dota de una herramienta electrónica a la policía judicial y a los fiscales para la investigación criminal, que ha contado con el apoyo técnico y logístico de los Estados Unidos, la misma que permite la posibilidad del monitoreo de llamadas, correos electrónicos, y todo lo que está inmerso dentro del espectro electromagnético de comunicaciones, siendo este proyecto uno, entre los que se deberían fomentar para el desarrollo de una política en pro de la persecución de la delincuencia informática, que permita el control integral de los delitos de índole tecnológico.

2.1.2.17 Organismos de Prevención de Delitos Informáticos a Nivel Mundial

En distintas latitudes del globo terráqueo se pueden encontrar distintas organizaciones que buscan la reducción de los Delitos Informático, debido al gran auge que han tenido en los últimos años, por lo que a continuación mencionaré algunas de estas agrupaciones, que deberían de existir en todo el mundo.

- La Guardia Civil Española es pionera en la investigación de delitos informáticos tendientes a su prevención. Allí, los guardiaciviles virtuales se encuentran con colegas de similares departamentos de las mejores policías del mundo tales como La Scotland Yard Británica, el FBI norteamericano, la PAF francesa o los herederos del KGB soviético, y otros agentes undercover de los servicios secretos de las potencias.

- En Estados Unidos ya florecen los investigadores privados que han sustituido el arma de fuego por el arma electrónica y que, en vez de "pies planos", empiezan a ser denominados "colas planas", pues casi toda la investigación la realizan a través de Internet, cómodamente sentados frente a su computadora.

- En Argentina La División computación de la Policía Federal conformado por doce efectivos a cargo del subcomisario Alberto Airala patrullan la red con el objeto de detectar los ilícitos que proliferan a través de ésta. Algunas veces lo hacen a requerimiento de instituciones y otras por expreso pedido de la justicia.

- El Grupo de Investigación en Seguridad y Virus Informáticos (G.I.S.V.I.), creado en la Universidad de Buenos Aires en 1995 actualmente funciona en la Universidad de Belgrano, ha resuelto varios casos de ataques de virus a empresas con características de acciones de sabotaje informático.

Es importante fomentar la creación de estas organizaciones, para que los usuarios no se vean invadidos en su privacidad, por lo que es un buen punto para comenzar con una buena legislación. [31]

2.1.2.18 Organismos Gubernamentales Ecuatorianos de Prevención de Delitos Informáticos

- Superintendencia de Bancos.

  Esta entidad está encargada de velar por la seguridad, estabilidad, transparencia y solidez de los sistemas financiero, de seguros privados y de seguridad social, mediante un eficiente y eficaz proceso de regulación y supervisión para proteger los intereses del público e impulsar el desarrollo del país.

- Superintendencia de Telecomunicaciones.

[31] **Derecho Informático, Dr. Julio Téllez Valdés, 2 ed. , México, McGrawHill**

Esta entidad está encargada de vigilar, auditar, intervenir y controlar técnicamente la prestación de los servicios de telecomunicaciones.

2.2 Marco Conceptual

2.2.1 Bomba lógica

Determinado programa o rutina que se activa al momento realizar una determinada acción, enviar un e-mail, ingresar a alguna aplicación, etc. Las bombas lógicas son consideradas virus informático. Normalmente su activación es oculta a los ojos del usuario y sus consecuencias varían: puede destruir la información del sistema, interceptar los servicios del sistema para propagarse a través del correo electrónico, etc.

2.2.2 Comunicación

Transmisión de mensajes entre personas. Como seres sociales las personas, además de recibir información de los demás, necesitamos comunicarnos para saber más de ellos, expresar nuestros pensamientos, sentimientos y deseos, coordinar los comportamientos de los grupos en convivencia, etc.

2.2.3 Delito informático

Crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.

2.2.4 Digitalización

Acción de convertir en digital información analógica. En otras palabras, es convertir cualquier señal de entrada continua en una serie de valores numéricos. Existen diferentes formas de digitalizar información, generalmente depende del tipo de información. Por ejemplo, una fotografía en papel suele digitalizarse empleando un escáner.

2.2.5 Estafa

Delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro.

2.2.6 Estafa Electrónica

Se trata de un anzuelo o estafa electrónica (phishing en inglés) que consiste en intentar adquirir información confidencial de forma fraudulenta.

Es un delito, que se comete mediante el uso de un tipo de ingeniería social. El estafador se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica: un correo electrónico, algún sistema de mensajería instantánea o, incluso, llamadas telefónicas.

2.2.7 Fraude

Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

2.2.8 Fraude Informático

Cualquier cambio no autorizado y malicioso de datos o informaciones contenido en un sistema informático.

2.2.9 HTML

Es un lenguaje de programación que se utiliza para el desarrollo de páginas de internet. Se trata de la sigla que corresponde a hypertext markup language, es decir, lenguaje de marcas de hipertexto.

2.2.10 Información

Datos que tienen significado para determinados colectivos. La información resulta

fundamental para las personas, ya que a partir del proceso cognitivo de la información que obtenemos continuamente con nuestros sentidos vamos tomando las decisiones que dan lugar a todas nuestras acciones.

2.2.11 Informática Forense

Se considera el uso de técnicas analíticas y de investigación para identificar, recopilar, analizar y preservar las pruebas / información que se almacena magnéticamente o codificado.

2.2.12 JavaScript

Es un lenguaje interpretado orientado a las páginas web, con una sintaxis semejante a la del lenguaje java.

2.2.13 Lavado de Dinero

Lavado de activos (la) son todas las acciones para dar apariencia de legalidad a recursos de origen ilícito. En la mayoría de los países del mundo ésta conducta es considerada delito y también se conoce como lavado de dinero, blanqueo de capitales, legitimación de capitales, entre otros.

2.2.14 Máquinas Zombis

Zombie es la denominación que se asigna a computadoras que tras haber sido infectadas por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo.

2.2.15 Multimedia

Cualquier sistema que utiliza múltiples medios de comunicación al mismo tiempo para presentar información. Generalmente combinan textos, imágenes, sonidos, videos y animaciones.

2.2.16 PGP

Pretty Good Privacy o PGP (privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

2.2.17 RDSI

Es una red que procede por evolución de la red telefónica existente, que al ofrecer conexiones digitales de extremo a extremo permite la integración de multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir y del equipo terminal que la genere.

2.2.18 Robo

Delito que se comete apoderándose con ánimo de lucro de una cosa mueble ajena, empleándose violencia o intimidación sobre las personas, o fuerza en las cosas.

2.2.19 Robo Informático

Delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos usando sistemas informáticos.

2.2.20 Sabotaje Informático

El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de uno (1) a seis (6) años y multa de cinco (5) a veinte (20) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

2.2.21 Seguridad Informática

Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

2.2.22 Tecnología

Aplicación de los conocimientos científicos para facilitar la realización de las actividades humanas. Supone la creación de productos, instrumentos, lenguajes y métodos al servicio de las personas.

2.2.23 Tecnologías de la Información y la Comunicación (TIC)

Cuando unimos estas tres palabras hacemos referencia al conjunto de avances tecnológicos que nos proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, internet, la telefonía, los "mas media", las aplicaciones multimedia y la realidad virtual. Estas tecnologías básicamente nos proporcionan información, herramientas para su proceso y canales de comunicación.

2.3 Formulación de la Hipótesis y Variables

2.3.1 Hipótesis General

Cada vez más personas se van resistiendo al uso de los servicios informáticos, por no existir acciones procedimentales, ni las herramientas para adquirir, preservar y recuperar evidencias digitales, además que los jueces no tienen adiestramiento para manejar estas evidencias que no son físicas sino intangibles.

2.3.2 Hipótesis Específicas

- No se cuenta con un alto nivel de conocimiento sobre las TICS, y esto influye en la cantidad de fraudes.

- Los autores de delitos informáticos en el país cuentan con un alto nivel de conocimiento sobre las TICS.

- No se cuenta con un buen nivel de seguridad en los servicios informáticos, por lo que cada vez las personas no lo usan.

- No se cuenta con procedimientos y planes bien establecidos para resolver los casos de delitos informáticos, por lo que cada vez aumentan más.

- Bajo las políticas actuales en el país, pocos casos de delitos informáticos se resuelven con éxito.

- El diseño de un nuevo esquema para prevenir y mejorar el proceso de indagación, podría reducirlos los delitos informáticos.

2.4 Matriz Causa – Efecto

FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL
¿Cuáles son las acciones procedimentales y recolección de evidencias a seguir contra los Delitos Informáticos en el Ecuador?	Establecer todas las formas de delito informático con herramientas tecnológicas mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los delitos informáticos.	Cada vez más personas se van resistiendo al uso de los servicios informáticos, por no existir acciones procedimentales, ni las herramientas para adquirir, preservar y recuperar evidencias digitales, además que los jueces no tienen adiestramiento para manejar estas evidencias que no son físicas sino intangibles.
SISTEMATIZACIÓN PROBLEMA	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICAS**
¿Cuáles son los mecanismos estadísticos y de juzgamiento empleados por el estado para resolver los delitos informáticos?	Establecer mecanismos procedimentales y de juzgamiento para ayudar a resolver los delitos informáticos.	No se cuenta con mecanismos procedimentales y de juzgamiento para resolver los delitos informáticos.
¿Dónde se dirigen las personas afectadas por los delitos informáticos?	Proponer funciones y requisitos mínimos para personal especializado en resolver los delitos informáticos.	Las personas no saben dónde dirigirse cuando existen casos de fraudes. Ya que el personal de la entidad no cuenta con funciones y requisitos mínimos para resolver los casos de delitos informáticos.
¿Cuentan los jueces con una visión clara sobre los delitos informáticos?	Establecer las características, parametrizar, encasillar los delitos informáticos.	Los jueces no cuentan con una visión clara sobre los delitos informáticos.
¿Cuentan con procedimientos y planes de acción para regular los delitos informáticos	Identificar los procedimientos y planes de acción para regular los delitos informáticos	No cuentan con procedimientos y planes de acción para regular los delitos informáticos.
¿Cómo se podría reducir los casos de delitos informáticos?	Identificar y analizar soluciones para reducir los casos de delitos	El diseño de un nuevo esquema que permita mejorar el proceso de

	informáticos.	indagación y resolución de los delitos informáticos.

Tabla 2.2 Matriz Causa-Efecto

Fuente: Autores

2.5 Variables

2.5.1 Variables Independientes

- Falta de procedimientos para resolver los delitos informáticos.

2.5.2 Variables Dependientes

- Cantidad de fraudes.

- Resistencia de las personas para el uso del comercio electrónico y transacciones con herramientas tecnológicas.

CAPÍTULO 3

ASPECTOS METODOLÓGICOS DE LA INVESTIGACIÓN

3.1 Tipo de Estudio

De acuerdo a la investigación que vamos a realizar y la propuesta que queremos presentar, vamos a utilizar los siguientes tipos de estudio:

- **Tipo de Investigación Exploratoria.-** Nuestra investigación se centra en determinar el impacto de los delitos informáticos en la administración de la justicia, y esta abarca diferentes áreas como: seguridad informática, legal, Tics, técnicas de hacking. De las cuales vamos encontrar una serie de fuentes de información que analizar y sintetizar para poder llegar a una conclusión correcta sobre el impacto de los delitos informáticos dándole un sentido a nuestra propuesta de solución.

- **Tipo de Investigación Descriptiva.-** Para el desarrollo de esta investigación y por sus características hemos decidido elegir la Investigación Descriptiva, que se utiliza cuando el proceso es de una complejidad tal que resulta necesario comenzar por describirlo del modo más riguroso posible, interesa realizarlo desde el marco descriptivo ya que ello posibilitará ocuparnos de la situación actual de la problemática en mención.

- **Tipo de Investigación Explicativa.-** Es una investigación de tipo explicativo porque se necesita encontrar y comprobar si las hipótesis planteadas son el verdadero motivo del aumento de los delitos informáticos, y plantear la mejor decisión para mejorar la situación actual con el diseño de un esquema para establecer un mejor uso de las Tics, para indagar y resolver de una manera eficaz los delitos informáticos.

- **Tipo de Investigación de Campo.-** La consideramos Investigación de Campo; con la realización de talleres de trabajo, entrevistas a miembros de la

Corte Superior de Justicia, personal del ministerio público, policía nacional y abogados en libre ejercicio; **cuestionarios** orientado a superar los problemas detectados.

Para lograr el objetivo, se considerarán los siguientes pasos:

Identificación de las características y cualidades del Especialista en tipificaciones de delitos con uso de las TICS en la administración de Justicia.

Detección de las principales causas de la falta de especialistas en tipificaciones de delitos con uso de las TICS en la administración de Justicia.

- **Tipo de Investigación Horizontal.-** Las diferentes variables, y situaciones serán analizadas en diferentes etapas de tiempo, desde el aparecimiento del problema y sus causas hasta la actualidad.

3.2 Métodos de Investigación

De acuerdo a la investigación que vamos a realizar y la propuesta que queremos presentar, vamos a utilizar los siguientes métodos de investigación.

- **Método Inductivo – Deductivo.-** Porque de las varias hipótesis e ideas debemos llegar a una conclusión, para poder establecer una solución al problema. De la misma forma de una conclusión concreta nos podemos basar para determinar de una mejor manera las partes particulares.

- **Método Analítico – Sintético.-** Nos guiaremos de otras investigaciones realizadas que giren en torno a nuestro tema para determinar fortalezas y debilidades a partir de experiencias anteriores.

  Se necesita establecer la relación causa y efecto entre las variables. Determinando como las variables influyen en los delitos informáticos. De acuerdo al desarrollo de la investigación podemos empezar por las variables al problema, o del problema a las variables.

- **Método Comparativo.-** Necesitamos usar la comparación entre los parámetro actuales y como mejoraría la situación actual con el esquema nuevo que vamos a diseñar.

- **Método Estadístico.-** Vamos usar el método estadístico para procesar las encuestas que vamos a realizar, necesitamos tabular datos, y hacer mediciones con estos.

3.3 Fuentes y Técnicas para la Recolección de Información

Las fuentes donde vamos a recolectar información es:

- En internet,
- En libros, periódicos,
- Entidad que resuelve delitos informáticos,
- Expertos sobre las TICS.

Las técnicas para recolectar información, serían las siguientes:

Realización de talleres de trabajo, entrevistas a miembros de la Corte Superior de Justicia, personal del ministerio público, y policía nacional; **cuestionarios** orientado a superar los problemas detectados.

- Para lograr el objetivo, se considerarán los siguientes pasos:
- Identificación de las tipificaciones de delitos.
- Detección de las principales causas de los problemas.
- Formulación de objetivos.
- Selección de las acciones de formación.
- Planificación.

3.4 Procedimientos de la Investigación

3.4.1 Aplicaciones

Descripción General

Se establecerá consenso sobre las siguientes acciones:

- Realización de la encuesta vía cuestionario acorde a la operacionalización de variables mencionadas.

- Establecer el conocimiento técnico de los miembros de las Instituciones de administración de Justicia necesarios para combatir esta clase de infracciones, así como los procedimientos y técnicas de investigación forense adecuadas para el examen de las evidencias encontradas.

3.4.2 Los Instrumentos

Siendo necesaria una aproximación multifocal para analizar el proceso en la administración de Justicia, el proceso de encuesta constará de cuatro formularios, cuyos resultados particulares deberán interpretarse dentro de un entramado, realizando el cruzamiento correspondiente:

- FORMULARIO 1 (F1): Cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia. (véase Anexo D)

- FORMULARIO 2 (F2): Cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia. (véase Anexo E)

- FORMULARIO 3 (F3): Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico del personal de las Instituciones de Administración de Justicia. (véase Anexo F)

- FORMULARIO 4 (F4): Cuestionario de conocimientos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informático al Público en General. (véase Anexo G)

Estos cuatros formularios integrarán la base de datos de cuestionarios.

- El **Cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia (F1)** se aplica en una instancia tal que implique la mayor cantidad de personal; de modo tal que se establezca como resultado el conocimiento en los mínimos requerimientos que necesita el personal de Administración de Justicia.

- El **Cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia (F2)** se aplica en una instancia tal que implique la mayor cantidad del personal que administra justicia en los ámbitos de las actividades delictivas, que debido a los cambios actuales se refiere a todas las instituciones penales de la Administración de Justicia y sus respectivos sujetos del proceso.

- El **Cuestionario de conocimientos técnicos Jurídicos sobre Informática, Telecomunicaciones y Comercio Electrónico (F3)** se aplica en una instancia tal que implique la mayor cantidad del personal que administra justicia en los ámbitos de las actividades delictivas, que debido a los cambios actuales se refiere a todas las instituciones penales de la Administración de Justicia.

- El **Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos(F4)** se aplica en una instancia tal que implique la mayor cantidad de personas de los distintos niveles sociales de la ciudad de Guayaquil que utilicen o podrían utilizar servicios informáticos.

3.4.3 Población y Muestra

La población para este proyecto está conformada por:

Área Jurídica – Guayaquil

Población:

Personal Corte de Justicia	78
Fiscalía General del estado	65
Policía Nacional	54
Abogados Libre Ejercicio	15000
Total	***15197***

Datos a diciembre del 2010

Público en General - Guayaquil

Población:

Casos de robos informáticos	**2.006**

Datos a abril del 2011

Expertos sobre las TICS.

- Para causar delitos informáticos. ***Entrevista con experto.***
    - ***Nombre: Ing. Roberto Olaya***
- Para resolver delitos informáticos. ***Entrevista con experto.***
    - ***Nombre: Ing. Roberto Olaya.***

3.4.4 Determinación de Números de Encuestas

Para el cálculo del tamaño de muestra, utilizamos la fórmula para una población conocida, la cual nos permite obtener un número representativo del grupo de personas que queremos estudiar.

La formula es la siguiente:

$n = (Z^2pqN) / (Ne^2 + Z^2pq)$

Donde:

n: muestra: es el número representativo del grupo de personas que queremos estudiar (población) y, por tanto, el número de encuetas que debemos realizar, o el número de personas que debemos encuestar.

N: población: es el grupo de personas que vamos a estudiar.

Z: nivel de confianza: mide la confiabilidad de los resultados. Lo usual es utilizar un nivel de confianza de 95% (1.96) o de 90% (1.65). Mientras mayor sea el nivel de confianza, mayor confiabilidad tendrán los resultados.

e: grado de error: mide el porcentaje de error que puede haber en los resultados. Lo usual es utilizar un grado de error de 5% o de 10%. Mientras menor margen de error, mayor validez tendrán los resultados.

p: probabilidad de ocurrencia: probabilidad de que ocurra el evento. Lo usual es utilizar una probabilidad de ocurrencia del 50%.

q: probabilidad de no ocurrencia: probabilidad de que no ocurra el evento. Lo usual es utilizar una probabilidad de no ocurrencia del 50%. La suma de “p” más “q” siempre debe dar 100%.

3.4.5 Obtención de la Muestra Área Jurídica y Público en General

Para el Personal Corte de Justicia, Fiscalía General del estado y Policía nacional se escogió una muestra estándar de 10 personas.

Para la muestra de los Abogados de Libre Ejercicio y Público en General por ser una población mayor se determinó por la utilización de la fórmula.

$n = (Z^2pqN) / (Ne^2 + Z^2pq)$

Donde:

Z=95%

e= 10%

p=50%

q=50%

Formulación para obtener muestra de los abogados de libre ejercicio:

$n = (1{,}96^2 * 0{,}5 * 0{,}5 * 15000) / (15000 * 0{,}05^2 + 1{,}96^2 * 0{,}5 * 0{,}5) = 95 \approx 70$

Quedando de la siguiente manera el número de muestras.

Área Jurídica – Guayaquil

Personal Corte de Justicia	10
Fiscalía General del estado	10
Policía Nacional	10
Abogados Libre Ejercicio	70
Total	***100***

Formulación para obtener muestra del público en general:

$n = (1{,}96^2 * 0{,}5 * 0{,}5 * 2006) / (2006 * 0{,}05^2 + 1{,}96^2 * 0{,}5 * 0{,}5) = 95 \approx 100$

Quedando de la siguiente manera el número de muestras.

Público en General - Guayaquil:

Personas que podrían utilizar los Servicios informáticos.	100

Vale la pena mencionar que una investigación de campo a este nivel no se ha realizado anteriormente.

3.4.6 Tratamiento de la Información

Con la Estadística vamos obtener resultados mediante determinadas reglas y operaciones. Este procedimiento los vamos a realizar a partir de los datos obtenidos de la encuesta y de las diferentes investigaciones. Los pasos serían los siguientes:

- Recuento, relevamiento o compilación datos,
- Tabulación y agrupamiento de datos. Representación gráfica,
- Medición de datos,
- Inferencia estadística. Predicción.

Una vez recopilados, ordenados y tabulados, los datos son analizados y procesados.

3.4.6.1 Recuento, Relevamiento o Recopilación de Datos

Consiste en la recolección de datos referidos a los delitos informáticos. Estos datos brindan información sobre las características de las variables que influyen en el problema.

3.4.6.2 Tabulación y Agrupamiento de Datos. Gráficos

Los datos recopilados son convenientemente ordenados, clasificados y tabulados mediante un software, que nos genera tablas que facilitan la lectura. Los gráficos permiten una interpretación simple y rápida de los hechos.

El software utilizado para la tabulación de datos forma parte de la plataforma de software especializada para la creación de estudios cuantitativos con instrumentos aplicados en campo (Papel, entrevistas telefónicas y entrevistas en dispositivos móviles) denominada “RotatorSurvey”.

Pasos generación de tablas y gráficos:

1. Creamos un estudio donde indicamos: nombre de estudio, palabra clave del estudio, código, nombre de nuestra organización, nombre de la organización de que se va a realizar el estudio, nombre y apellido del que va a realizar el estudio, el login, correo y contraseña.

2. Indicamos en que carpeta se desea guardar el estudio.

3. Diseñamos los cuestionarios.

4. Creamos las preguntas que están en el cuestionario, donde colocamos el código de la pregunta, la descripción, tipo de pregunta, nombre corto para el análisis, y palabra clave.

5. Gerenciamos la carga de datos, ingresamos los cuestionarios, ya sea en forma tipiado o entrevista.

6. Compilamos la información, salimos para ingresar al Analizador.

7. En el Analizador OLAP de Estudios, escogemos el estudio creado, en la lista de sugerencia que nos muestra el software.

8. Nos dirigimos a Tabulador masivo, y nos muestras las tablas y gráficos de las preguntas ingresadas.

9. Realizamos arreglos de forma de presentación.

10. Presentamos resultados.

3.4.6.3 Medición de Datos

Se realiza la elaboración matemática y medición de los datos. Se observa que los datos tienden a centrarse en torno de ciertos valores llamados parámetros o medidas de posición (promedio, mediana, moda).
Luego se analiza la dispersión de los datos con respecto a esos valores centrales, se definen entonces los parámetros o medidas de dispersión (desvíos, desviación estándar).

3.4.6.4 Inferencia Estadística. Predicción

Mediante los datos obtenidos se plantean conclusiones y se predicen el comportamiento futuro de las variables entorno al problema.

3.4.7 Operacionalización de Variables

VARIABLE	ÁMBITOS	DIMENSIONES	INDICADOR
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	Jurídico TICS Informática jurídica	TICS Análisis forense	Conocimientos sobre: Informática Forense, Análisis Forense digital, Manejo de Evidencias Digitales, Peritaje TICS.

Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	Jurídico TICS	TICS Normas jurídicas	Conocimientos sobre: Ley de Comercio Electrónico, Ley de Telecomunicaciones, Ley de Propiedad Intelectual, Ley de Transparencia y Acceso a la Información.
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	Jurídico TICS	TICS	Conocimientos sobre: Infracciones Informáticas.
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	Jurídico TICS	TICS	Conocimientos sobre el Procedimiento penal de los delitos Informáticos

Tabla 3.1a Cuadro de Operacionalización de Variables 1

Fuente: Autores

VARIABLE	ÁMBITOS	DIMENSIONES	INDICADOR
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	TICS	Telecomunicaciones	Conocimientos sobre : Redes, Telefonía Digital, Video
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	TICS	Informática	Conocimientos sobre : Uso de Computador personal - Uso de Internet - Uso de Equipos Inalámbricos Uso de Celulares u otros dispositivos
Falta de procedimientos e incidencia de la falta de formación de los especialistas en los delitos informáticos en la Administración de Justicia en la Sociedad Ecuatoriana e Identificación de los retos y brechas que debe ser superada por la Administración de Justicia en la Sociedad Ecuatoriana con sede en Guayaquil para el tratamiento de los mismos.	TICS	Comercio electrónico	Conocimientos sobre : Transferencias Electrónicas, Documentos Digitales

Tabla 3.1b Cuadro de Operacionalización de Variables

Fuente: Autores

3.4.8 Resultados e Impactos Esperados

De la investigación y el diagnóstico de la Situación Actual esperamos obtener datos cuantitativos y estándar. La información más completa sobre:

- Tecnologías y Estrategias empleadas por las Autoridades que resuelven los casos de Delitos Informáticos.

- Procesos y procedimientos actuales, en el caso que hubiere, empleados por las Autoridades para resolver los delitos informáticos.

- Tecnologías y Estrategias empleadas por las personas que cometen delitos informáticos.

Mediante la información obtenida de la investigación se desea establecer:

- Características, parametrizar, encasillar los delitos informáticos.

- Funciones y requisitos mínimos para personal especializado en resolver los delitos informáticos.

- Mecanismos procedimentales y de juzgamiento para ayudar a resolver los delitos informáticos.

Esperamos establecer de forma clara el impacto de los Delitos Informáticos con herramientas tecnológicas mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los mismos.

Con la propuesta del Diseño de nuevo esquema para el procedimiento de indagación de los delitos informáticos, se espera:

- Disminuir la resistencia de las personas al usar los servicios informáticos.

- Ayudar con el desarrollo del país en el ámbito tecnológico.

- Disminuir las pérdidas millonarias principalmente en el sector bancario.

- Disminuir los delitos informáticos.

CAPÍTULO 4

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Procesamiento y Análisis

Concluida la aplicación de los instrumentos, se procedió a la tabulación de las respuestas y sus resultados se presentan de manera sistemática en cuadros estadísticos, considerando las frecuencias con sus respectivos porcentajes, los cuales permiten visualizar de manera numérica la información. Además, son presentados en gráficos estadísticos.

La interpretación de los resultados se realizó de la siguiente manera:

- **Cuantitativos.** Los resultados numéricos son convertidos en porcentajes, considerando cada uno de los ítems.

- **Cualitativos.** En base a los porcentajes obtenidos, se realizó el respectivo análisis para obtener las conclusiones, lo cual permitió objetividad en cuanto a los resultados de la investigación.

4.1.1 Aplicación y Procesamiento de Datos

Los Resultados

La información obtenida del trabajo de campo permitirá el análisis de los resultados de la encuesta al personal de las Instituciones de Administración de Justicia, a los Abogados en Libre Ejercicio y al Público en General. De la misma forma se analizara las respuestas de la entrevista a los expertos en causar y resolver delitos informáticos.

Se obtuvo los resultados de todos los formularios a fin de obtener una comprensión global del fenómeno en estudio.

RESULTADOS FORMULARIO 1 (F1): Cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

1. ¿Usted tiene conocimiento de computación?

	P1 Usted tiene conocimiento de computación	(1) SI	57
		(2) EN PARTE	20
		(3) NO	14
		(4) N/C	9
		Total Base sujetos (Conocimiento computación)	100

Tabla 4.1 Cuadro de Resultado de Conocimiento de Computación
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

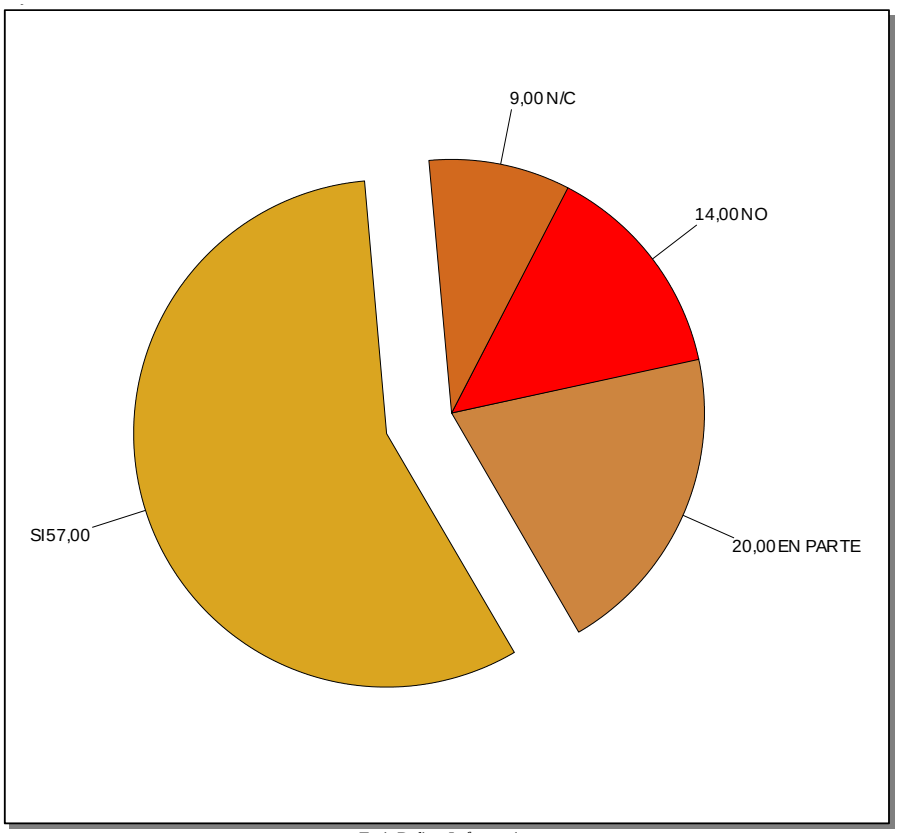


Figura 4.1 Gráfico de Resultado de Conocimiento de Computación
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 23 % que no tenían conocimientos básicos de computación; mientras un 77 % manifestaron que no es así. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla

curricular desde los niveles más básicos de estudios informáticos para la población de áreas jurídicas que por su elevada edad tienen esta falencia.

2. ¿Maneja usted un computador personal?

	P2 Maneja usted un computador personal	(1) SI	60
		(2) EN PARTE	21
		(3) NO	11
		(4) N/C	8
		Total Base sujetos (Computador)	100

Tabla 4.2 Cuadro de Resultado de Manejo de Computador Personal
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

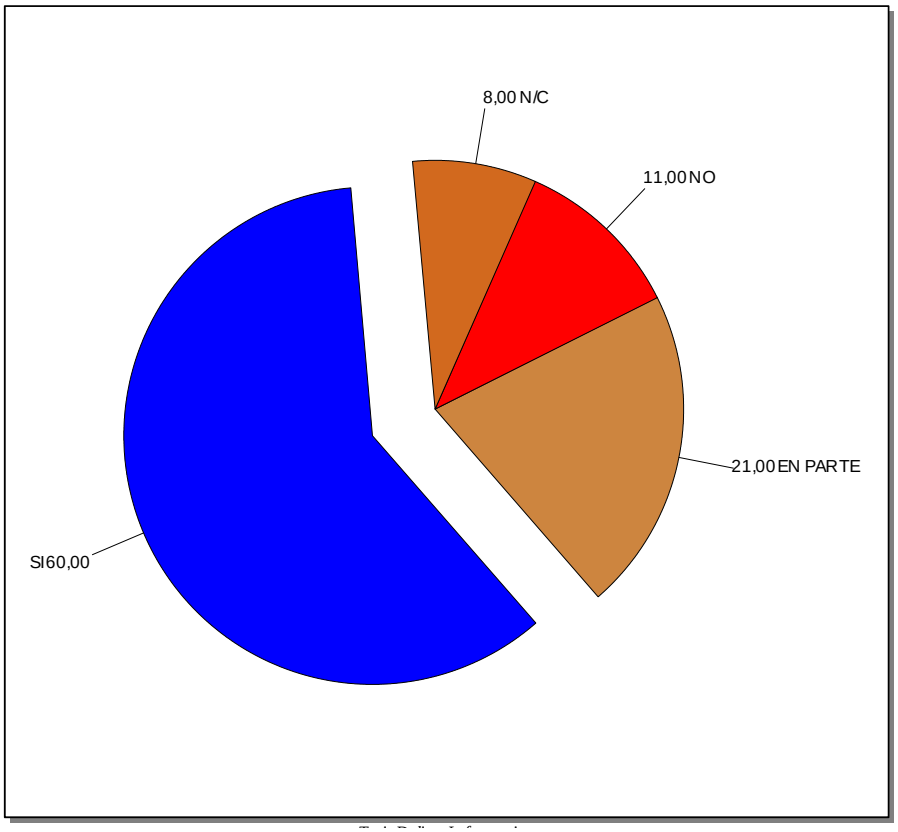


Figura 4.2 Gráfico de Resultado de Manejo de Computador Personal
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 19 % que no tenían experiencia en manejo de un Computador Personal; mientras un 81 % manifestaron que si tenían experiencia. Las Instituciones tecnológicas Superiores deben orientar su

planificación y malla curricular desde los niveles más básicos de estudios informáticos para la población de áreas jurídicas que por su elevada edad tienen esta falencia.

3. ¿Conoce sobre la herramienta de internet?

	P3 Conoce sobre la herramienta de internet	(1) SI	59
		(2) EN PARTE	21
		(3) NO	12
		(4) N/C	8
		Total Base sujetos (Herramienta de internet)	100

Tabla 4.3 Cuadro de Resultado de Uso de Herramientas de Internet
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

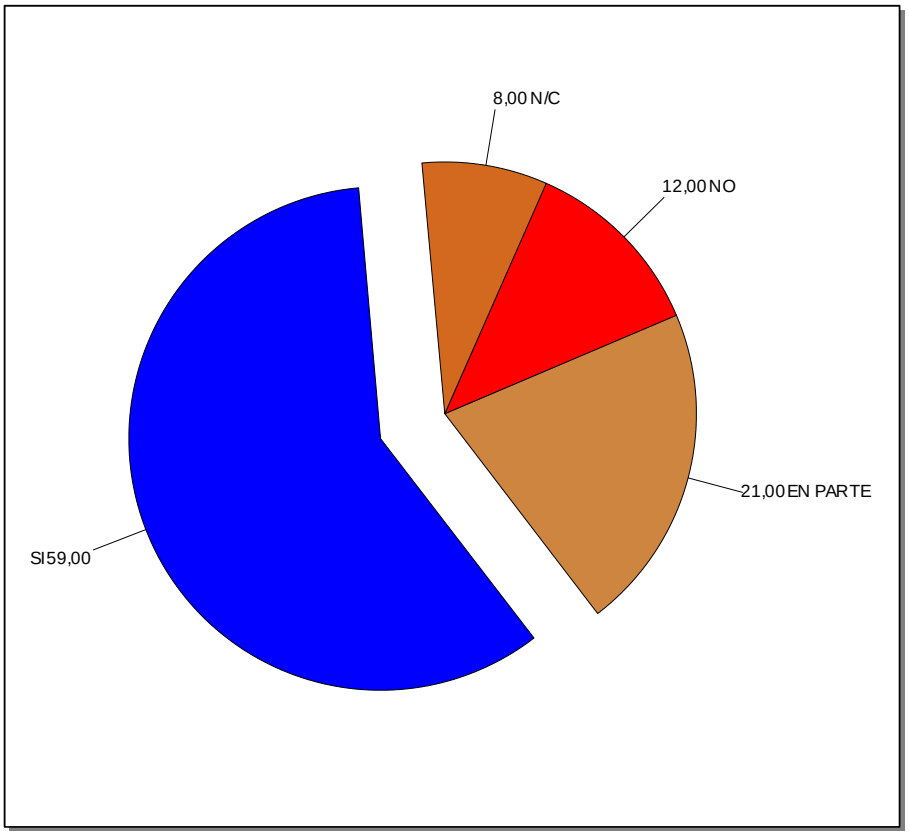


Figura 4.3 Gráfico de Resultado de Uso de Herramientas de Internet
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 20 % que no tenían conocimientos de herramientas de Internet; mientras un 80 % manifestaron que si

tenían conocimiento. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular desde los niveles más básicos de conocimientos de entornos y herramientas de internet para la población de áreas jurídicas que por su elevada edad tienen esta falencia.

4. ¿Maneja internet?

	P4 Maneja internet	(1) SI	58
		(2) EN PARTE	18
		(3) NO	13
		(4) N/C	11
		Total Base sujetos (Maneja internet)	100

Tabla 4.4 Cuadro de Resultado de Experiencia en Manejo de Internet
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

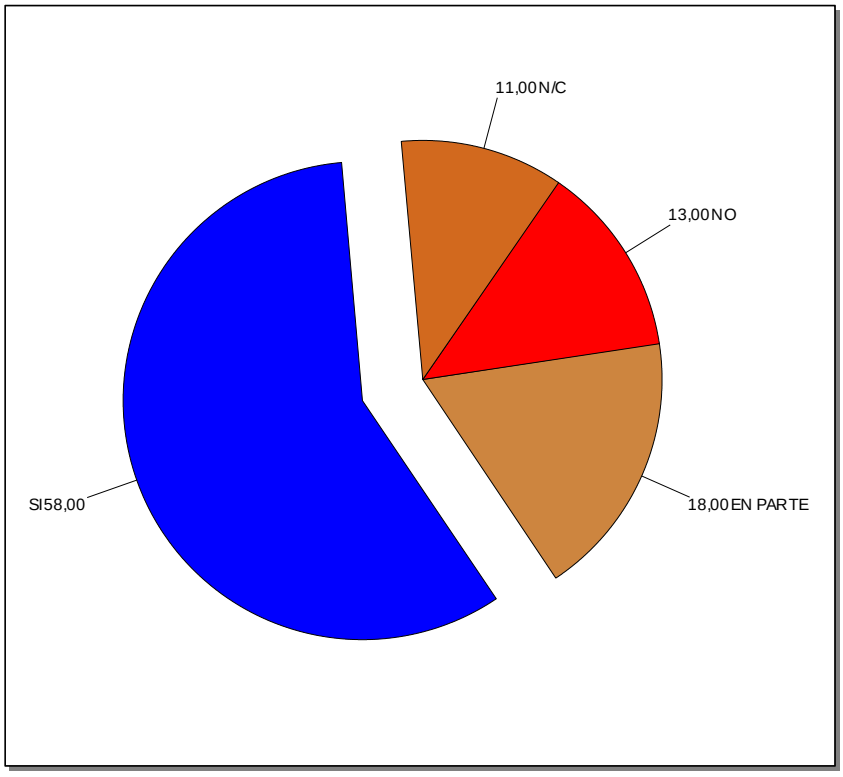


Figura 4.4 Gráfico de Resultado de Experiencia en Manejo de Internet
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 29 % que no tenían experiencia en manejo de entornos de Internet; mientras un 71 % manifestaron que si

tenían experiencia. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular desde los niveles más básicos de conocimientos de entornos y herramientas de internet para la población de áreas jurídicas que por su elevada edad tienen esta falencia.

5. ¿Conoce sobre los delitos informáticos?

	P5 Conoce sobre los delitos informáticos	(1) SI	52
		(2) EN PARTE	24
		(3) NO	16
		(4) N/C	8
		Total Base sujetos (Informáticos)	100

Tabla 4.5 Cuadro de Resultado de Conocimientos sobre Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

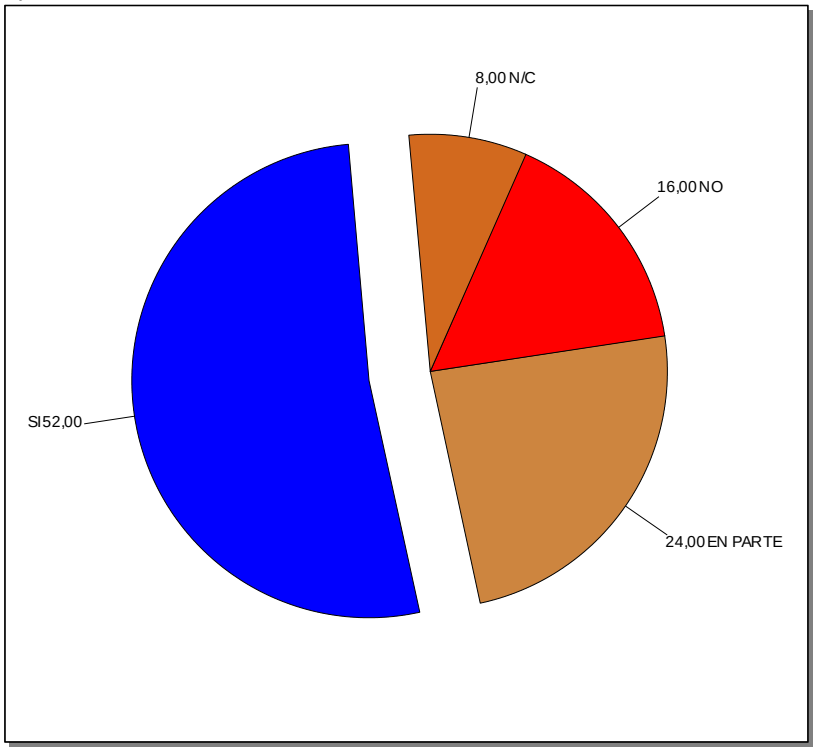


Figura 4.5 Gráfico de Resultado de Conocimientos sobre Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 24 % que no tenían conocimiento de Delitos Informáticos; mientras un 76 % manifestaron que si tenían

conocimiento. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

6. ¿Sabe cuáles son los principales delitos informáticos?

	P6 Sabe cuales son los principales delitos informáticos	(1) SI	37
		(2) EN PARTE	31
		(3) NO	24
		(4) N/C	8
		Total Base sujetos (Informáticos)	100

Tabla 4.6 Cuadro de Resultado de Principales Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

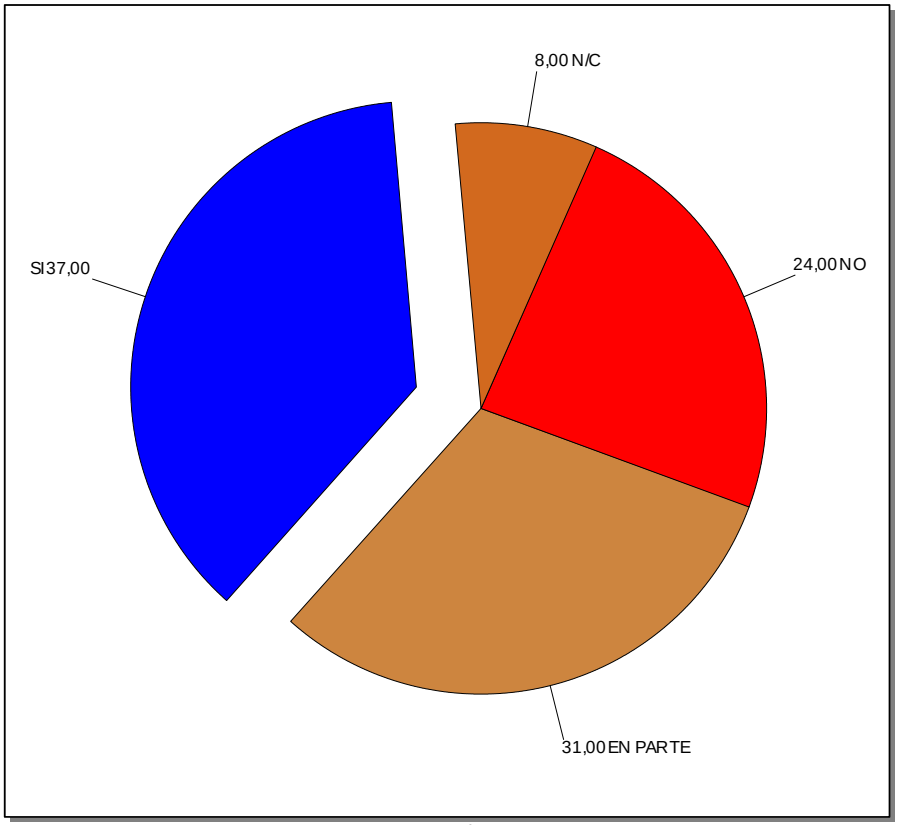


Figura 4.6 Gráfico de Resultado de Principales Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 32 % que no tenían

conocimiento de los principales Delitos Informáticos que afectan a nuestra actual sociedad en la Administración de Justicia; mientras un 68 % manifestaron que si tenían conocimiento. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

7. ¿Conoce el marco legal que los regula?

	P7 Conoce el marco legal que los regula	(1) SI	21
		(2) EN PARTE	27
		(3) NO	44
		(4) N/C	8
		Total Base sujetos (Conoce regula)	100

Tabla 4.7 Cuadro de Resultado de Marco Legal que regula los Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

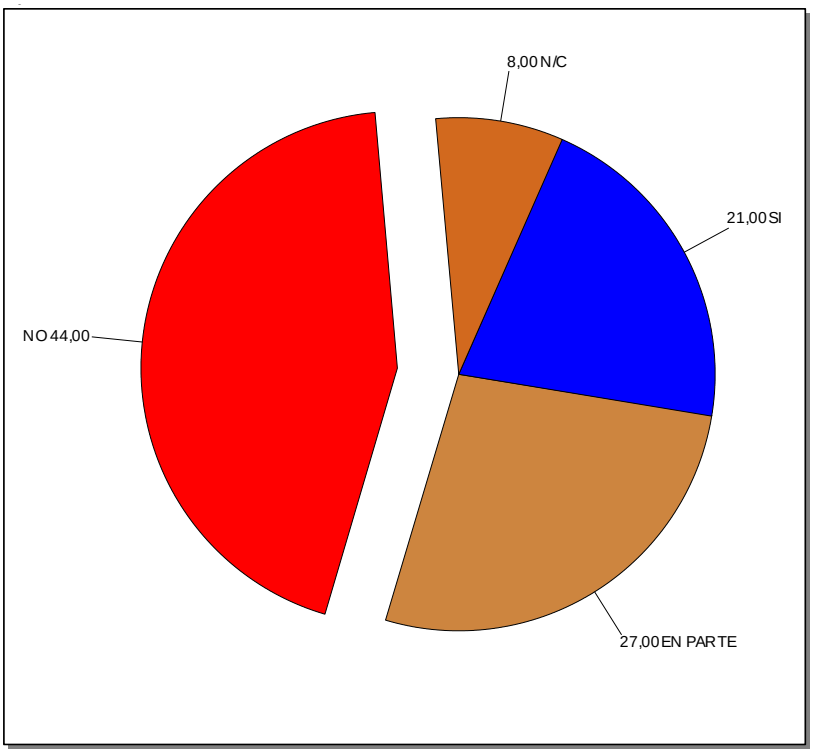


Figura 4.7 Gráfico de Resultado de Marco Legal que regula los Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 52 % que no tenían conocimiento del Marco Jurídico de los Delitos Informáticos que afectan a nuestra actual sociedad en la Administración de Justicia; mientras un 48 % manifestaron que si tenían conocimiento.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento del marco Jurídico de los Delitos utilizando las TICS que ocurren en la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

8. ¿Conoce el delito informático más común?

	P8 Conoce el delito informático más común	(1) SI	47
		(2) EN PARTE	19
		(3) NO	24
		(4) N/C	10
		Total Base sujetos (Informático)	100

Tabla 4.8 Cuadro de Resultado de Delito Informático más común en la Sociedad Ecuatoriana
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

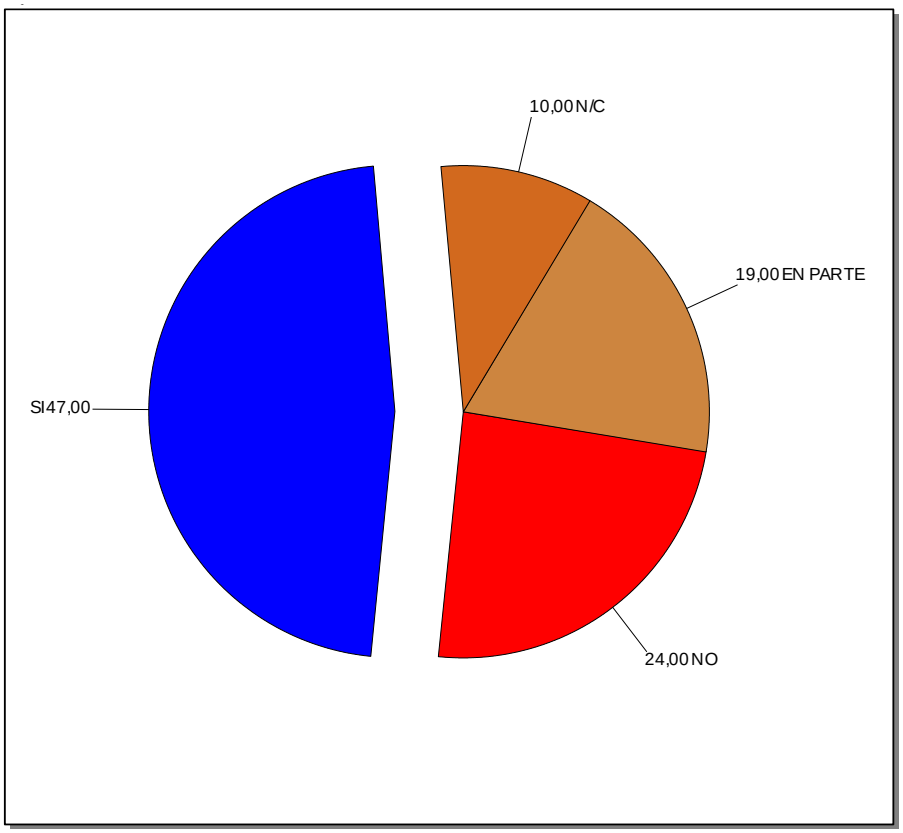


Figura 4.8 Gráfico de Resultado de Delito Informático más común en la Sociedad Ecuatoriana
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 34 % que no tenían conocimiento de cuál es el Delito Informático tipificado más recurrente que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 66 % manifestaron que si tenían conocimiento.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

9. ¿Sabe dónde las personas encargadas de estos delitos se capacitan?

	P9 Sabe dónde las personas encargadas de estos delitos se capacitan	(1) SI	22
		(2) EN PARTE	15
		(3) NO	54
		(4) N/C	9
		Total Base sujetos (Encargadas de estos)	100

Tabla 4.9 Cuadro de Resultado de Capacitación en Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

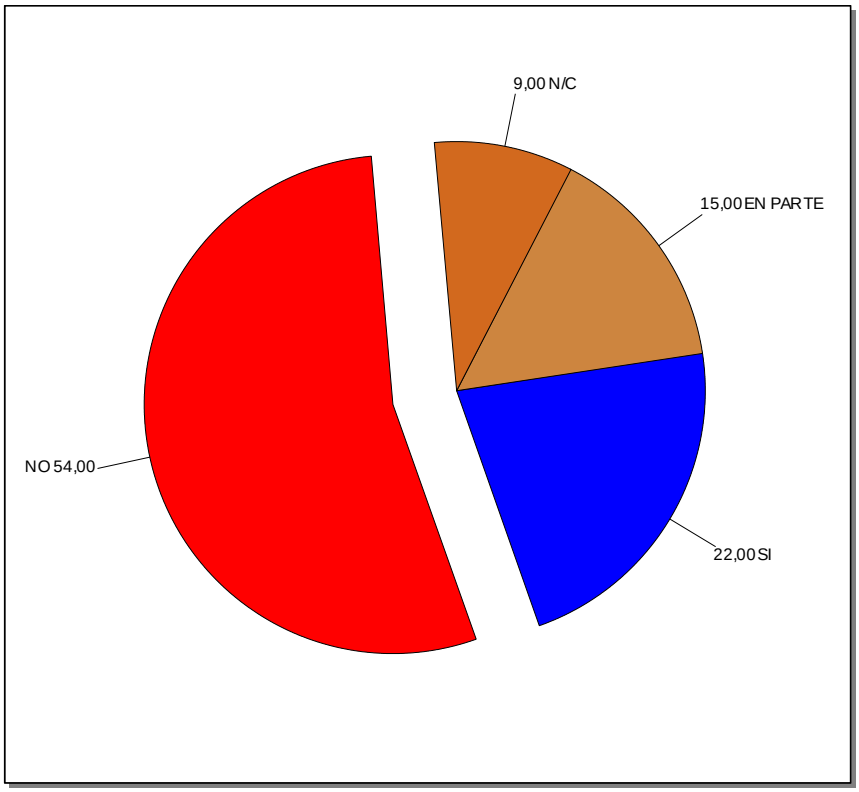


Figura 4.9 Gráfico de Resultado de Capacitación en Delitos Informáticos
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 63 % que no tenían conocimiento de dónde se realiza capacitaciones sobre los Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 37 % manifestaron que si tenían conocimiento.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los

Delitos utilizando las TICS que necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

10. ¿Ha recibido capacitación sobre los delitos informáticos?

	P10 Ha recibido capacitación sobre los delitos informáticos	(1) SI	19
		(2) EN PARTE	16
		(3) NO	54
		(4) N/C	11
		Total Base sujetos (Capacitación informáticos)	100

Tabla 4.10 Cuadro de Resultado de Capacitación
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

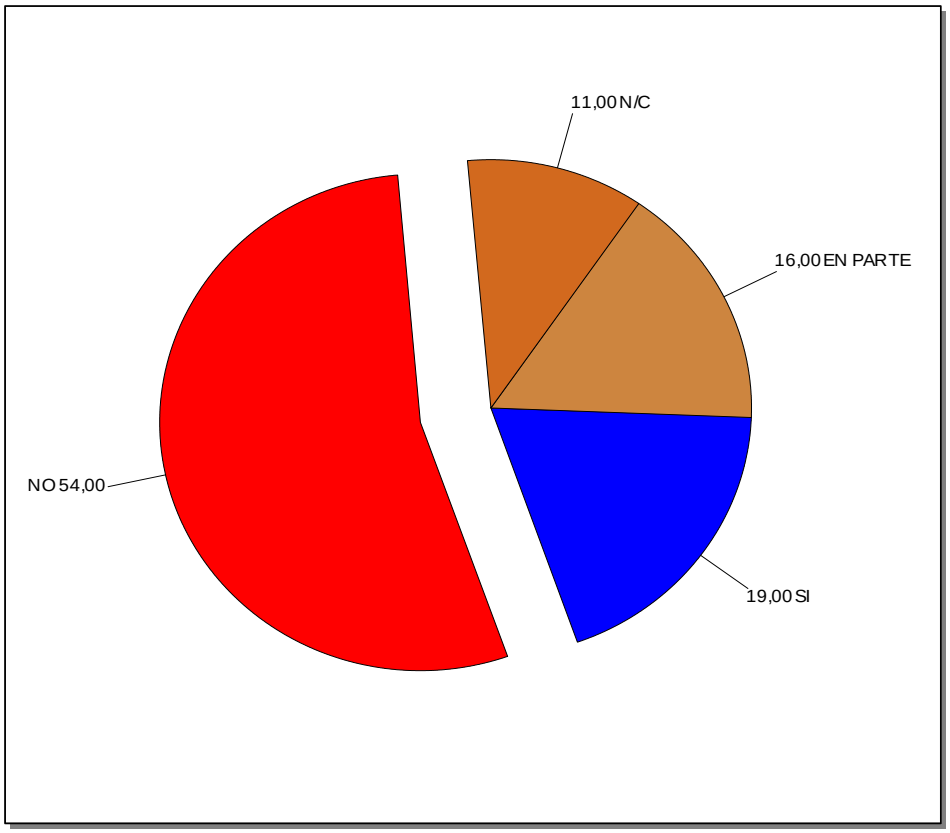


Figura 4.10 Gráfico de Resultado de Capacitación
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 65 % que no han recibido capacitaciones sobre los Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 35 % manifestaron que si han

recibido capacitación. Dado este resultado es indispensable que las instituciones tecnológicas superiores orienten y especialicen a los capacitados en el reconocimiento y formas de atención de los Delitos utilizando las TICS que necesita la sociedad; dado la falta de capacitación en un área que está en continuo desarrollo.

11. ¿Conoce usted qué es la seguridad informática?

	P11 Conoce usted qué es la seguridad informática	(1) SI	20
		(2) EN PARTE	26
		(3) NO	44
		(4) N/C	10
		Total Base sujetos (Informática)	100

Tabla 4.11 Cuadro de Resultado de Conocimiento sobre Seguridad Informática
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

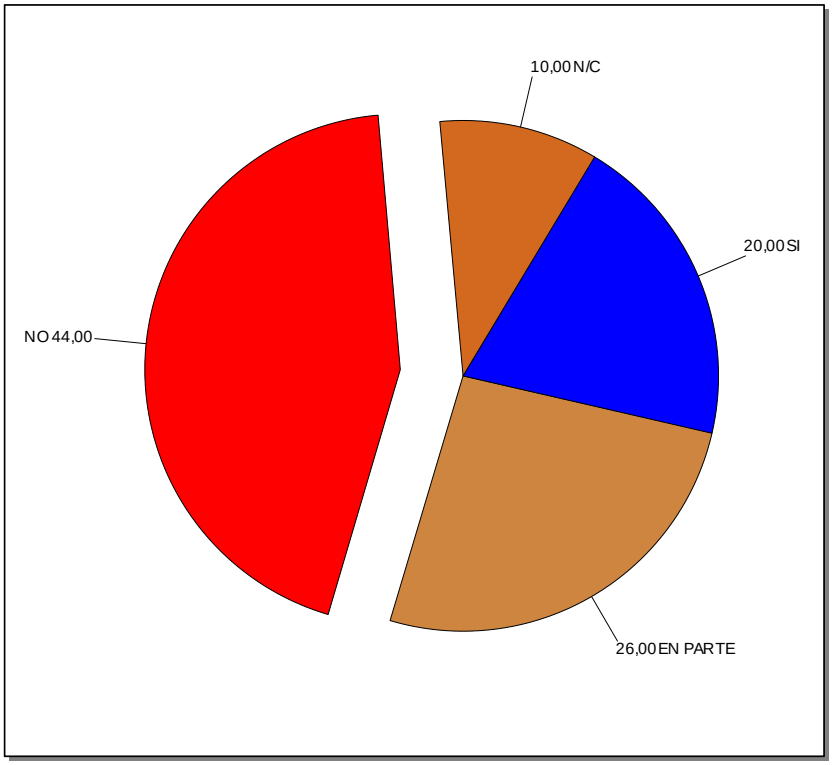


Figura 4.11 Gráfico de Resultado de Conocimiento sobre Seguridad Informática
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 54 % que no conocen lo referente a Seguridad Informática que incide directamente en los Delitos utilizando

las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 46 % manifestaron que si tienen conocimiento.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

12. ¿Toma acciones para evitar delitos informáticos?

	P12 Toma acciones para evitar delitos informáticos	(1) SI	22
		(2) EN PARTE	19
		(3) NO	49
		(4) N/C	10
		Total Base sujetos (Informáticos)	100

Tabla 4.12 Cuadro de Resultado de Toma de Acciones para evitar Delito Informático
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

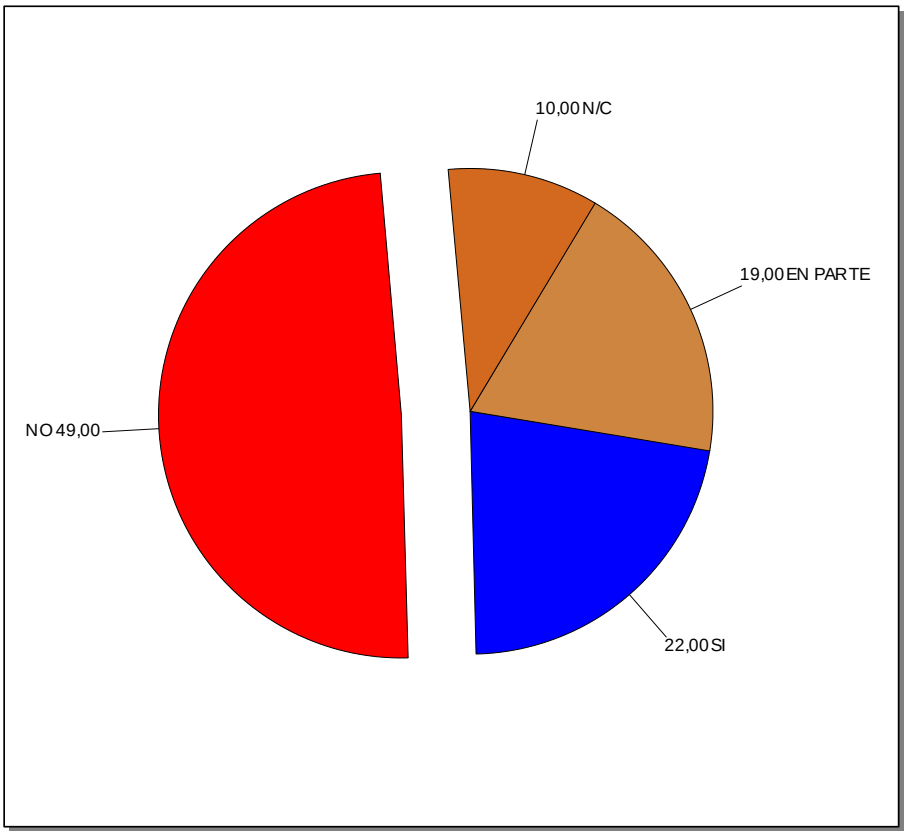


Figura 4.12 Gráfico de Resultado de Toma de Acciones para evitar Delito Informático
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 59 % no toma acciones para evitar Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 41 % manifestaron que si tomaban acciones de prevención.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

13. ¿Conoce alguna actividad cotidiana en el computador que se considere delito?

	P13 Conoce alguna actividad cotidiana en el computador que se considere delito	(1) SI	22
		(2) EN PARTE	18
		(3) NO	49
		(4) N/C	11
		Total Base sujetos (Cotidiana actividad)	100

Tabla 4.13 Cuadro de Resultado de Actividad Cotidiana que se considere Delito Informático
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

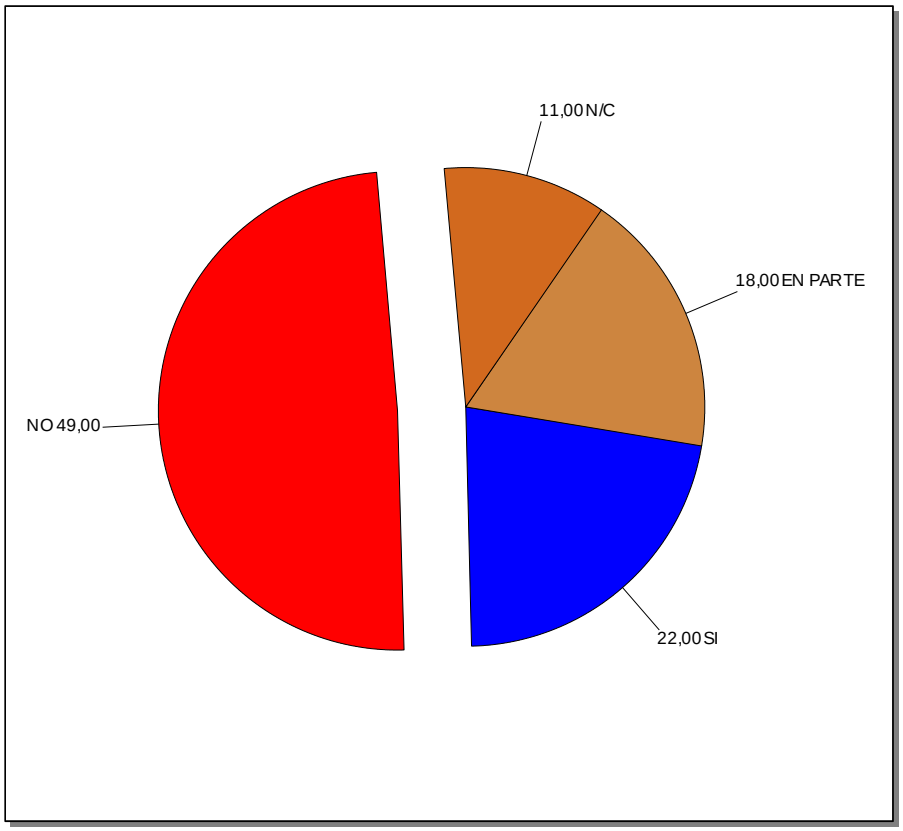


Figura 4.13 Gráfico de Resultado de Actividad Cotidiana que se considere Delito Informático
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 60 % no conoce si existen actividades que se realicen cotidianamente y se consideren Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras

un 40 % manifestaron que si conocían de este tipo de actividades. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

14. ¿Conoce usted cómo se procede en un delito informático?

	P14 Conoce usted cómo se procede en un delito informático	(1) SI	19
		(2) EN PARTE	23
		(3) NO	49
		(4) N/C	9
		Total Base sujetos (Informático)	100

Tabla 4.14 Cuadro de Resultado de Conocimiento del Procedimiento en los Delitos con uso de las TICS
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

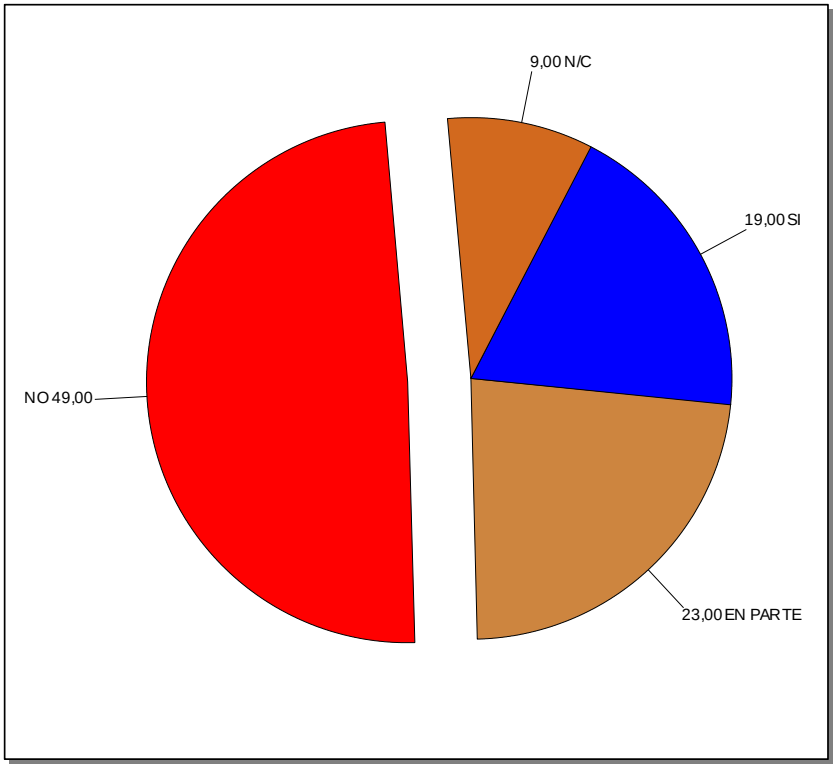


Figura 4.14 Gráfico de Resultado de Conocimiento del Procedimiento en los Delitos con uso de las TICS
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 58 % no conoce el procedimiento para la gestión de justicia en los casos de Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 42 % manifestaron que si conocen el procedimiento a utilizar.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

15. ¿Sabe usted como resguardar evidencias digitales?

	P15 Sabe usted como resguardar evidencias digitales	(1) SI	22
		(2) EN PARTE	19
		(3) NO	49
		(4) N/C	10
		Total Base sujetos (Resguardar evidencias)	100

Tabla 4.15 Cuadro de Resultado de Forma de Resguardar Evidencias Digitales
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

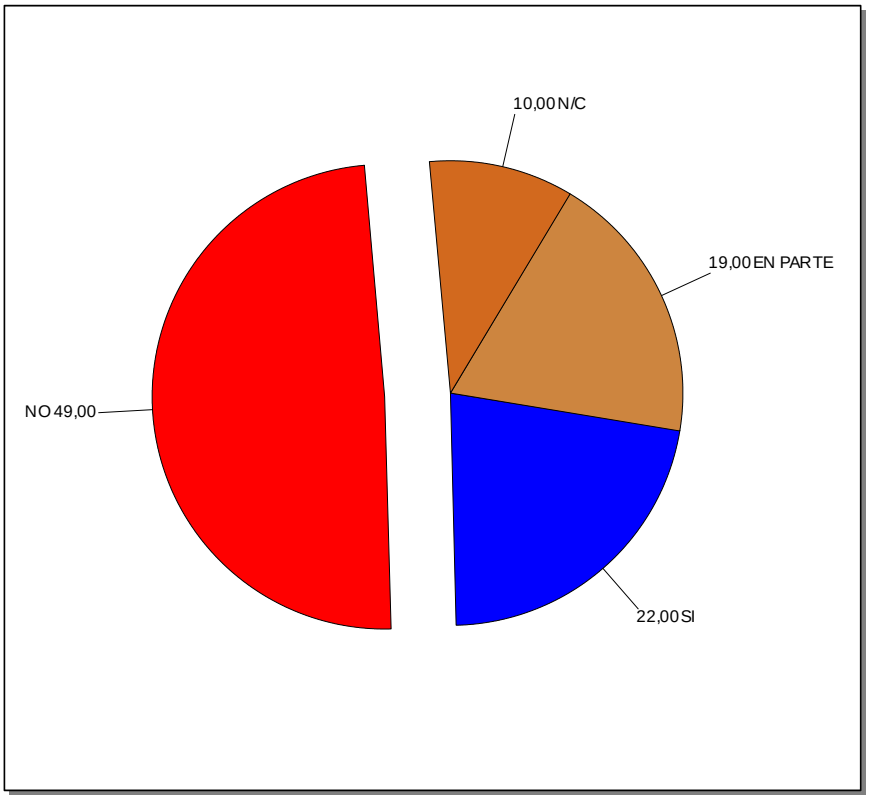


Figura 4.15 Gráfico de Resultado de Forma de Resguardar Evidencias Digitales Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 59 % que no conoce la forma de resguardar evidencia digital para la gestión de justicia en los casos de Delitos utilizando las TICS que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 41 % manifestaron que si conocen el procedimiento a utilizar.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

16. ¿Conoce usted qué es una Firma Electrónica?

	P16 Conoce usted qué es una Firma Electrónica	(1) SI	46
		(2) EN PARTE	19
		(3) NO	25
		(4) N/C	10
		Total Base sujetos (Electrónica)	100

Tabla 4.16 Cuadro de Resultado de Conocimiento de Firmas Electrónicas
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

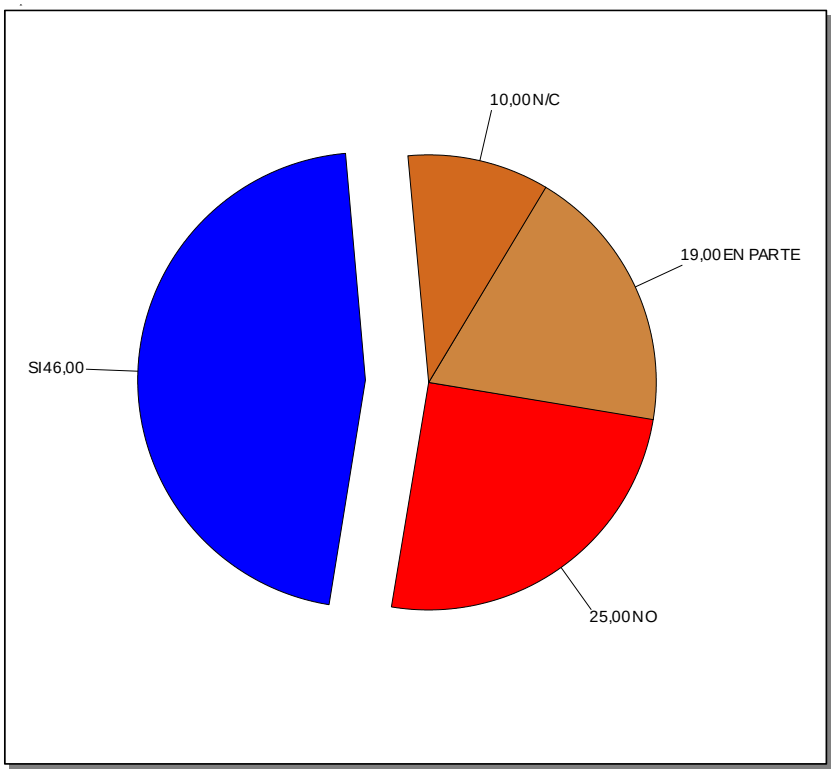


Figura 4.16 Gráfico de Resultado de Conocimiento de Firmas Electrónicas
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron en 35 % que no conoce ni posee información respecto a la Firma Electrónica como elemento vinculado a las TICS y que constituye un nuevo servicio de Seguridad con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 65 % manifestaron que si están actualizados con la temática de Firma Electrónica.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla

curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

17. ¿Ha realizado una transacción electrónica?

	P17 Ha realizado una transacción electrónica	(1) SI	49
		(2) EN PARTE	21
		(3) NO	22
		(4) N/C	8
		Total Base sujetos (Transacción electrónica)	100

Tabla 4.17 Cuadro de Resultado de Uso de Transacciones Electrónicas
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

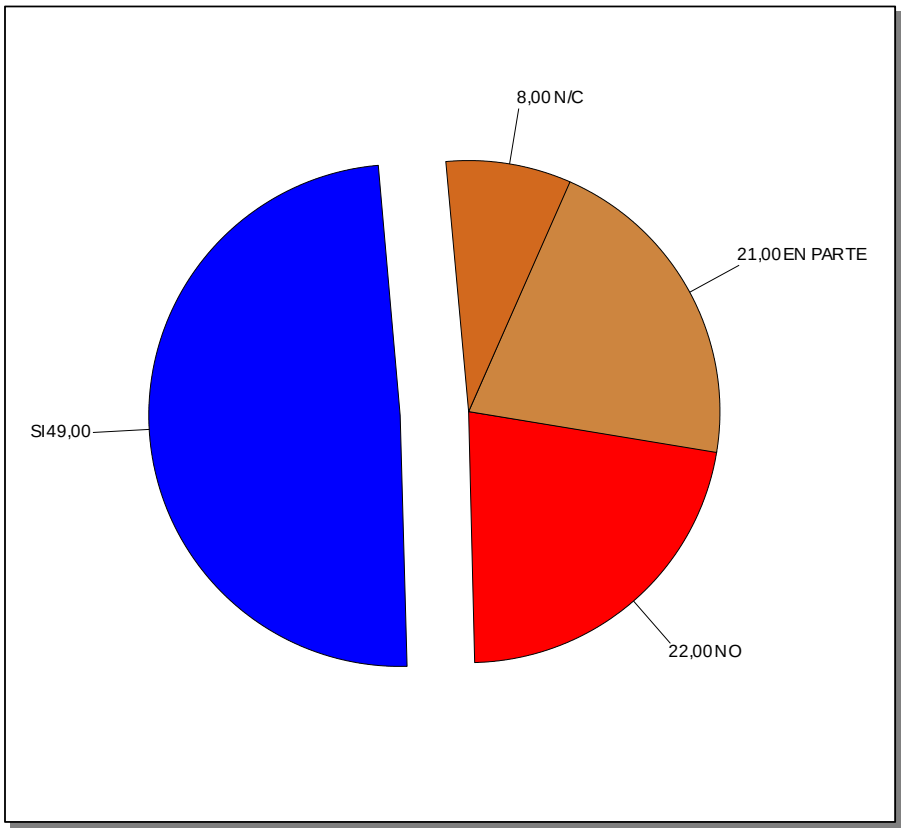


Figura 4.17 Gráfico de Resultado de Uso de Transacciones Electrónicas
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 30 % que no conoce ni ha realizado transacciones electrónicas en los Portales de Internet como elemento vinculado a las TICS y que constituye un nuevo servicio comercial con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 70 % manifestaron que si toman precauciones al momento de realizar actividades en Comercio Electrónico

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

18. ¿Ha tomado precauciones al realizar transacciones digitales?

	P18 Ha tomado precauciones al realizar transacciones digitales	(1) SI	28
		(2) EN PARTE	16
		(3) NO	48
		(4) N/C	8
		Total Base sujetos (Precauciones transacciones)	100

Tabla 4.18 Cuadro de Resultado de Prevención en Comercio Electrónico
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

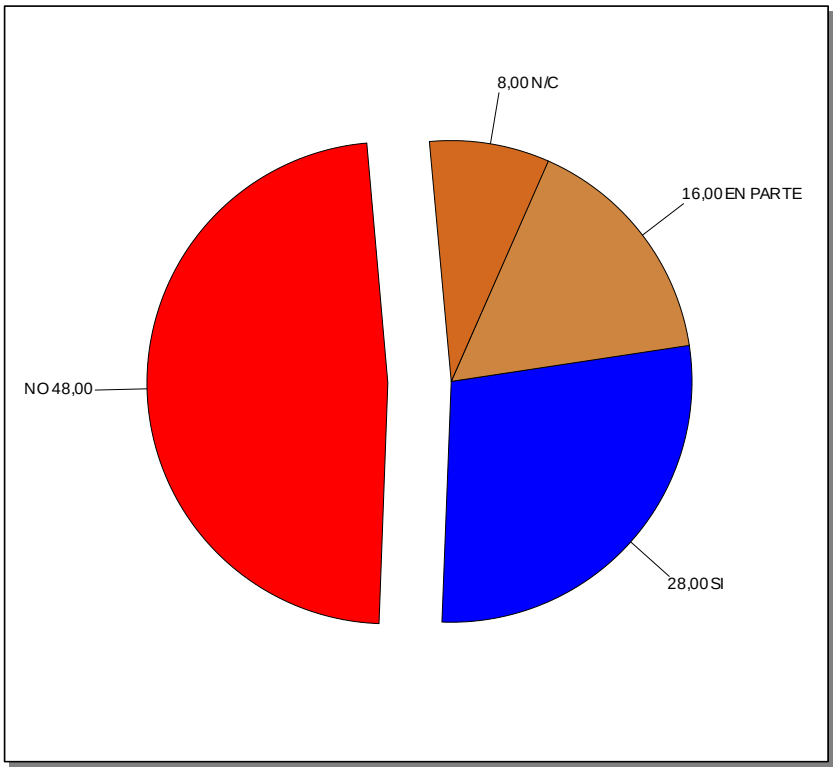


Figura 4.18 Gráfico de Resultado de Prevención en Comercio Electrónico
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 56 % que no toma medidas de precaución ni de prevención al momento de realizar transacciones electrónicas en los Portales de Internet como elemento vinculado a las TICS y que constituye un nuevo servicio comercial con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 44 % manifestaron que si toman medidas de prevención.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

19. ¿Conoce la Factura Electrónica?

	P19 Conoce la factura electrónica	(1) SI	23
		(2) EN PARTE	17
		(3) NO	52
		(4) N/C	8
		Total Base sujetos (Electrónica)	100

Tabla 4.19 Cuadro de Resultado de Conocimiento de Factura Electrónica
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

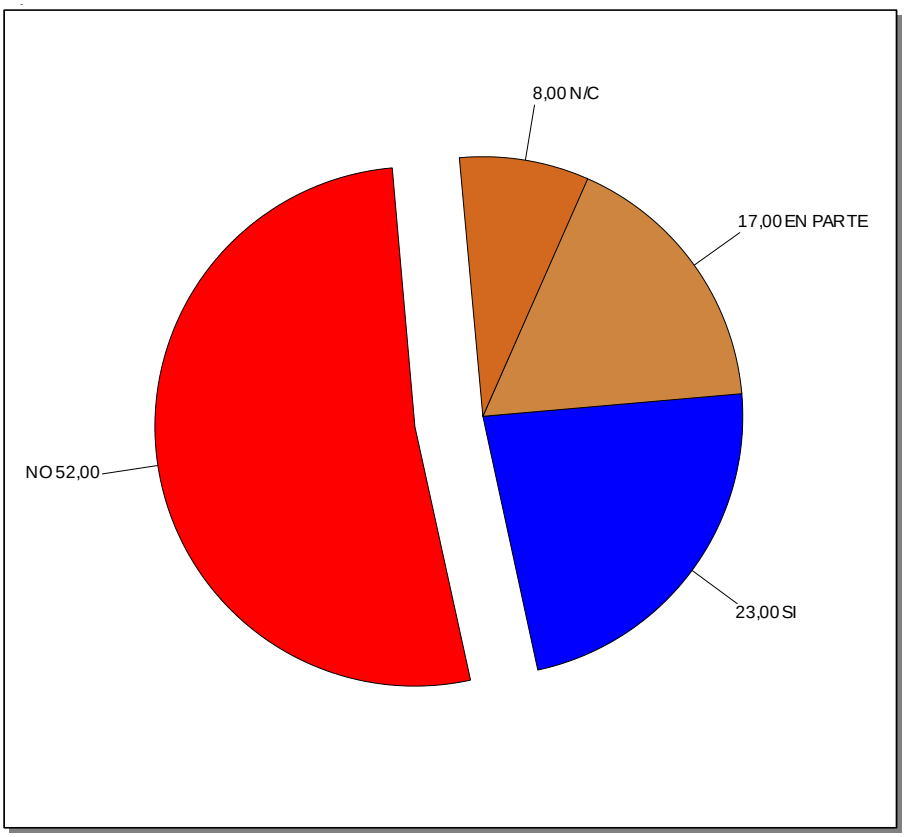


Figura 4.19 Gráfico de Resultado de Conocimiento de Factura Electrónica
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 60 % que no conocen ni poseen información sobre el nuevo proceso de Facturación Electrónica en el Ecuador al momento de realizar transacciones electrónicas comerciales en los Portales de Internet o en cualquier intercambio comercial y que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 40 % manifestaron que si poseen conocimientos sobre la

Facturación Electrónica. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

20. ¿Tiene usted Correo Electrónico?

	P20 Tiene usted Correo Electrónico	(1) SI	60
		(2) EN PARTE	16
		(3) NO	14
		(4) N/C	10
		Total Base sujetos (Correo electrónico)	100

Tabla 4.20 Cuadro de Resultado de Uso de Correo Electrónico
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

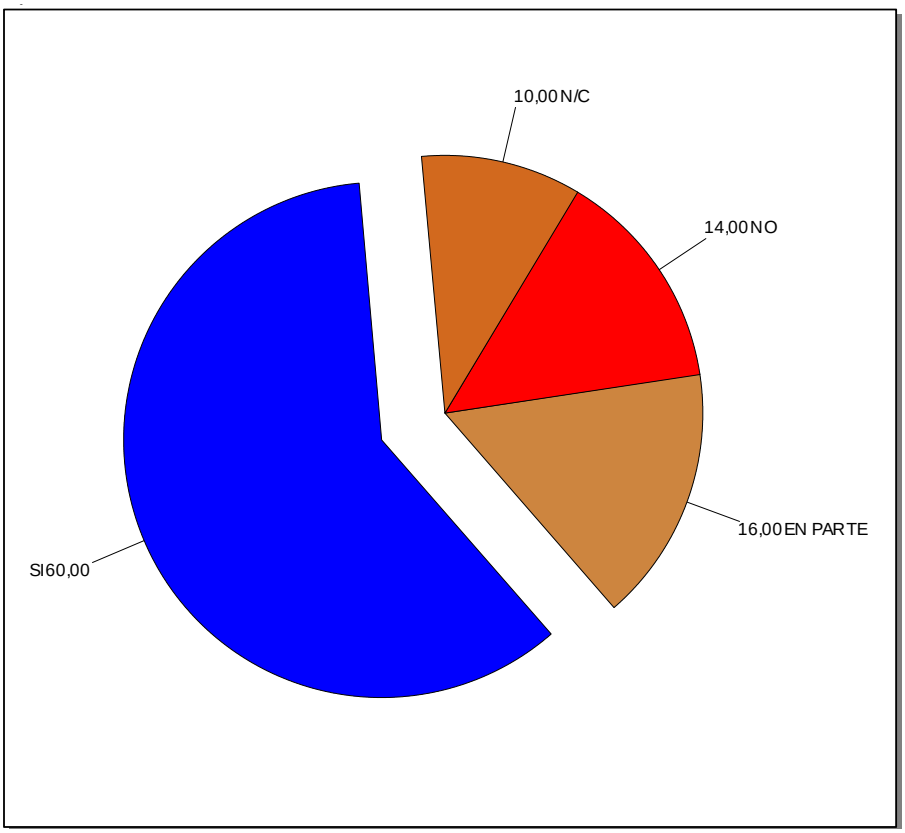


Figura 4.20 Gráfico de Resultado de Uso de Correo Electrónico
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 24 % que no posee un correo electrónico ni personal ni corporativo y que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 76 % manifestaron que si toman medidas de prevención.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

RESULTADOS FORMULARIO 2 (F2): Cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

1. Delitos contra elementos físicos (Hardware): robo, hurto, estafa, apropiación indebida y daños.

	P1 Delitos contra elementos fisicos (Hardware): robo, hurto, estafa, apropiación indebida y daños.	(1) SI	57
		(2) EN PARTE	24
		(3) NO	14
		(4) N/C	4
		{VACIO}	>
		Total Base sujetos (Apropiación)	100

Tabla 4.21 Cuadro de Resultado de Delitos contra elementos físicos (Hardware): robo, hurto, estafa, apropiación indebida y daños

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

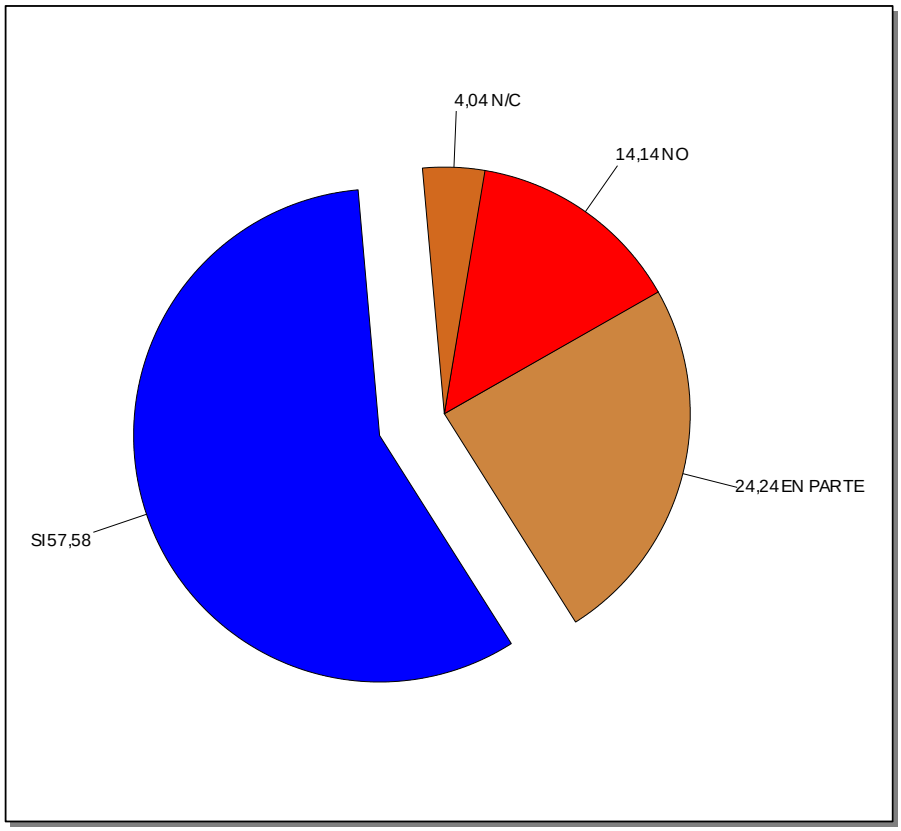


Figura 4.21 Gráfico de Resultado de Delitos contra elementos físicos (Hardware): robo, hurto, estafa, apropiación indebida y daños
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 19 % que no posee conocimientos sobre el marco legal del daño y acceso ilícito a Hardware y Software y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 81 % manifestaron que si tienen conocimiento de esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

2. Delitos contra elementos lógicos (Software).

	P2 Delitos contra elementos lógicos .	(1) SI	34
		(2) EN PARTE	17
		(3) NO	42
		(4) N/C	7
		Total Base sujetos (Elementos)	100

Tabla 4.22 Cuadro de Resultado de Daños en sistemas o elementos lógicos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

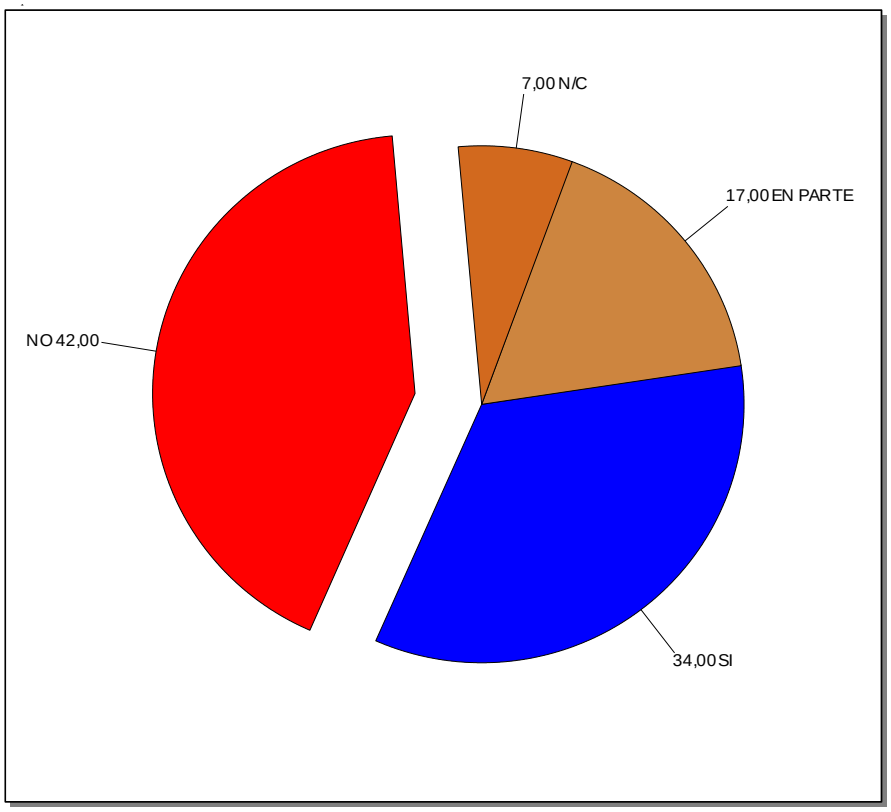


Figura 4.22 Gráfico de Resultado de Daños en sistemas o elementos lógicos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 46 % que no posee conocimientos sobre el marco legal del daño y acceso ilícito a Software y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 54 % manifestaron que si tienen conocimiento de esta temática. Las Instituciones tecnológicas Superiores deben

orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones; sobre todo debido a que es un área que está en continuo desarrollo.

3. Daños en sistemas o elementos informáticos, (Art 6 Ley de Comercio Electrónico) en datos, programas o documentos electrónicos (sabotaje informático).

	P3 Daños en sistemas o elementos informáticos, (Art 6 Ley de Comercio Electrónico) en datos, programas o documentos electrónicos (sabotaje informático).	(1) SI	23
		(2) EN PARTE	43
		(3) NO	32
		(4) N/C	2
		Total Base sujetos (Electrónicos)	100

Tabla 4.23 Cuadro de Resultado de Daños en sistemas
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

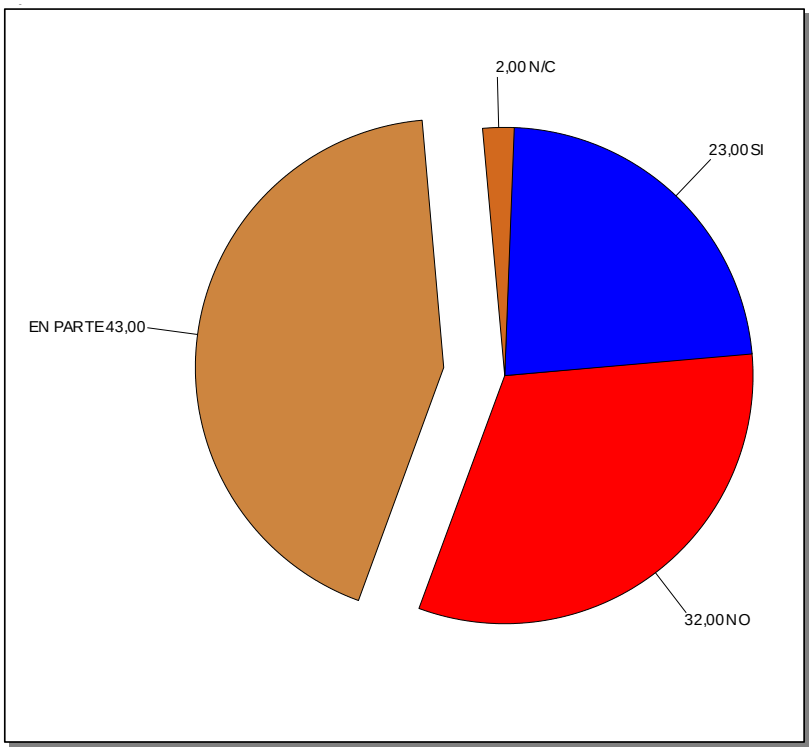


Figura 4.23 Gráfico de Resultado de Daños en sistemas
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 53 % que no posee conocimientos sobre el acceso no autorizado utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 66 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

4. Acceso ilícito a sistemas informáticos (secretos, derecho a la intimidad, protección de datos, propiedad intelectual e industrial).

	P4 Acceso ilícito a sistemas informáticos (secretos, derecho a la intimidad, protección de datos, propiedad intelectual e industrial).	(1) SI	35
		(2) EN PARTE	27
		(3) NO	28
		(4) N/C	10
		Total Base sujetos (Informáticos)	100

Tabla 4.24 Cuadro de Resultado de Daños y Acceso ilícito a sistemas informáticos

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

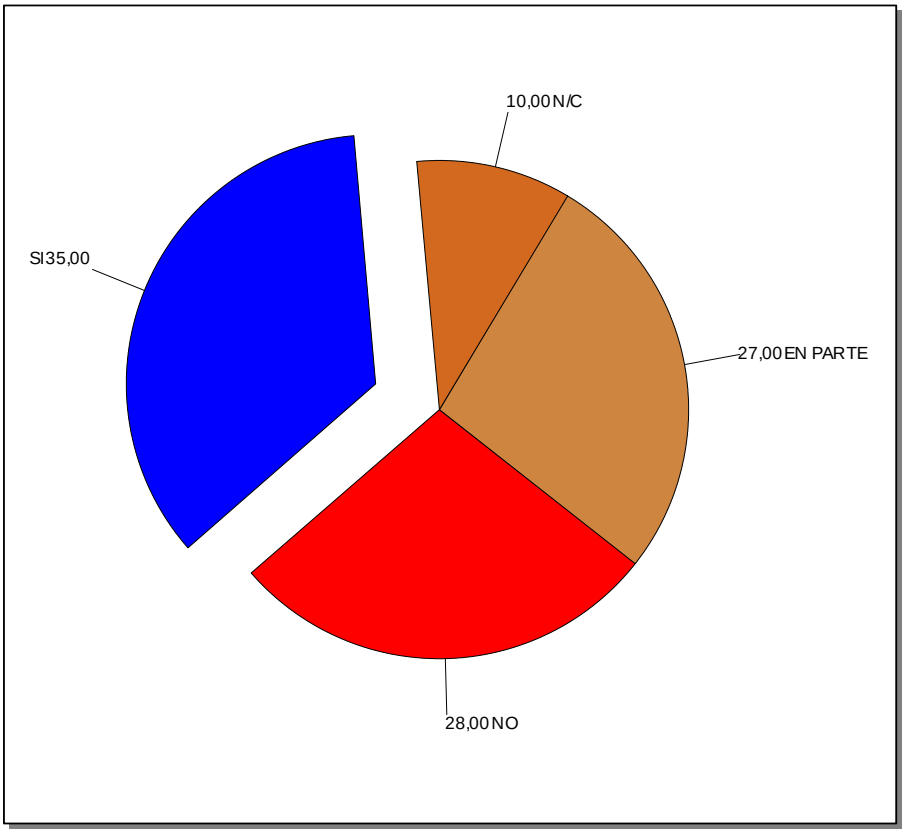


Figura 4.24 Gráfico de Resultado de Daños y Acceso ilícito a sistemas informáticos

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 38 % que no posee conocimientos sobre el marco legal del daño y acceso ilícito a Hardware y Software y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 62 % manifestaron que si tienen conocimiento de esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

5. Acceso no autorizado a sistemas informáticos ajenos, utilizando las redes públicas de telefonía o transmisión de datos, burlando las medidas de seguridad, como contraseñas o claves de acceso.

	P5 públicas de telefonía o transmisión de datos, burlando las medidas de seguridad, como contraseñas o claves de acceso.	(1) SI	32
		(2) EN PARTE	18
		(3) NO	42
		(4) N/C	8
		Total Base sujetos (Contraseñas o claves)	100

Tabla 4.25 Cuadro de Resultado de Hacking
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

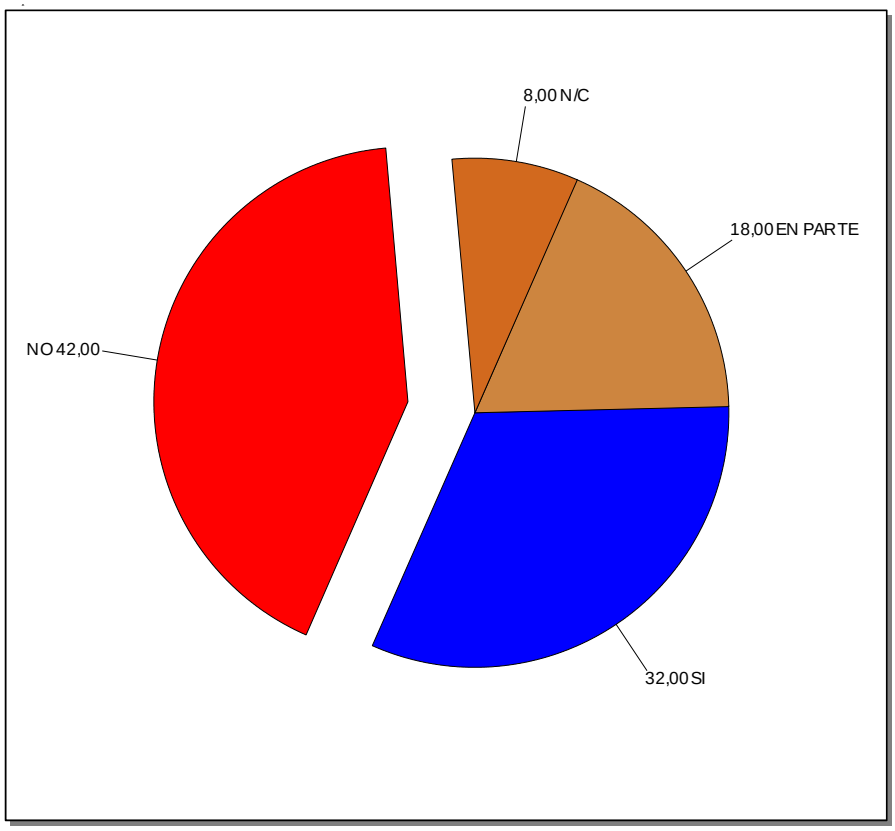


Figura 4.25 Gráfico de Resultado de Hacking
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 50 % que no posee conocimientos sobre el acceso no autorizado utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la

Administración de Justicia; mientras un 50 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

6. Las finalidades del hacking.

	P6 Finalidades del hacking.	(1) SI	26
		(2) EN PARTE	15
		(3) NO	50
		(4) N/C	9
		Total Base sujetos (Finalidades hacking)	100

Tabla 4.26 Cuadro de Resultado de las finalidades del hacking
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

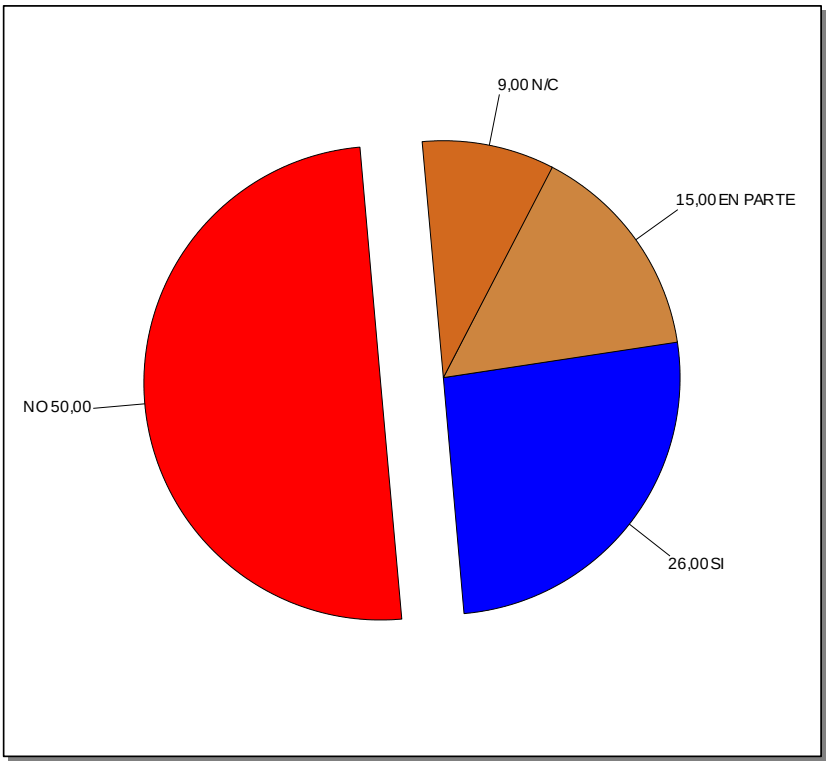


Figura 4.26 Gráfico de Resultado de las finalidades del hacking
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 59 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 41 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

7. Accesos ilícitos a datos que pueden considerarse secretos de empresa.

	P7 Accesos ilícitos a datos que pueden considerarse secretos de empresa.	(1) SI	29
		(2) EN PARTE	15
		(3) NO	47
		(4) N/C	9
		Total Base sujetos (Considerarse)	100

Tabla 4.27 Cuadro de Resultado de Accesos ilícitos a datos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

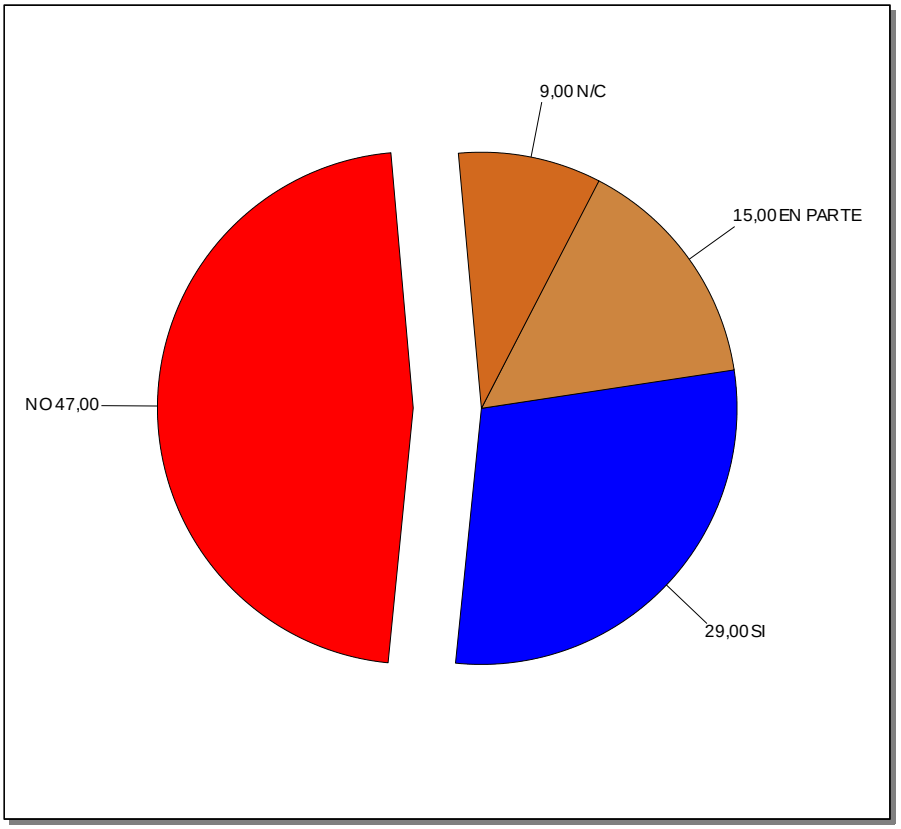


Figura 4.27 Gráfico de Resultado de Accesos ilícitos a datos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 56 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 44 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben

orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

8. Datos que se califican de secretos.

	P8 Datos que se califican de secretos	(1) SI	28
		(2) EN PARTE	17
		(3) NO	45
		(4) N/C	10
		Total Base sujetos (Califican de secretos)	100

Tabla 4.28 Cuadro de Resultado de Datos que se califican de secretos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

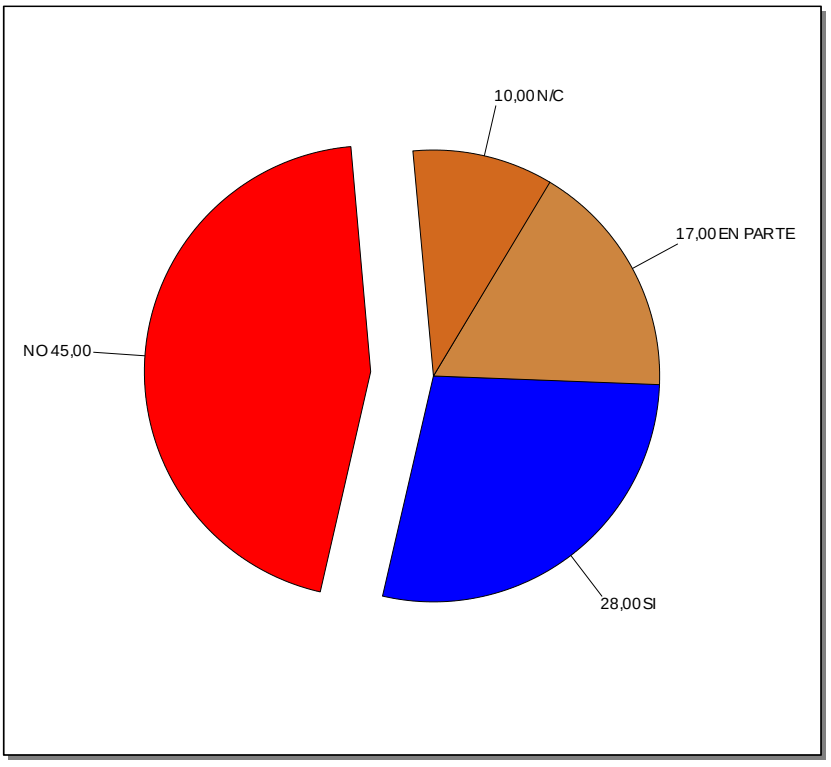


Figura 4.28 Gráfico de Resultado de Datos que se califican de secretos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 55 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 45% manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

9. Procedimientos de fabricación o de investigación de nuevos productos.

	P9 Procedimientos de fabricación o de investigación de nuevos productos.	(1) SI	24
		(2) EN PARTE	18
		(3) NO	50
		(4) N/C	8
		Total Base sujetos (Investigación procedimientos)	100

Tabla 4.29 Cuadro de Resultado de Procedimientos de fabricación
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

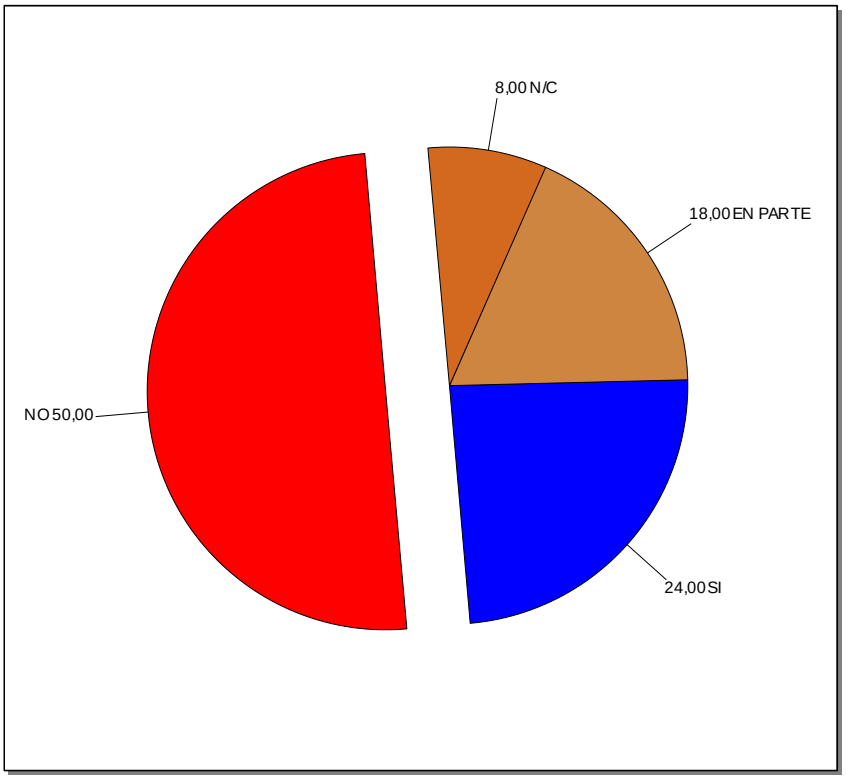


Figura 4.29 Gráfico de Resultado de Procedimientos de fabricación
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 58 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 42 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

10. Lista de clientes, tarifas, descuentos, distribuidores, estrategias comerciales, modelo de negocio, modo de trabajo, proyectos de expansión.

	P10 Lista de clientes, tarifas, descuentos, distribuidores, estrategias comerciales, modelo de negocio, modo de trabajo, proyectos de expansión.	(1) SI	22
		(2) EN PARTE	18
		(3) NO	51
		(4) N/C	9
		Total Base sujetos (Proyectos expansión)	100

Tabla 4.30 Cuadro de Resultado de Datos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

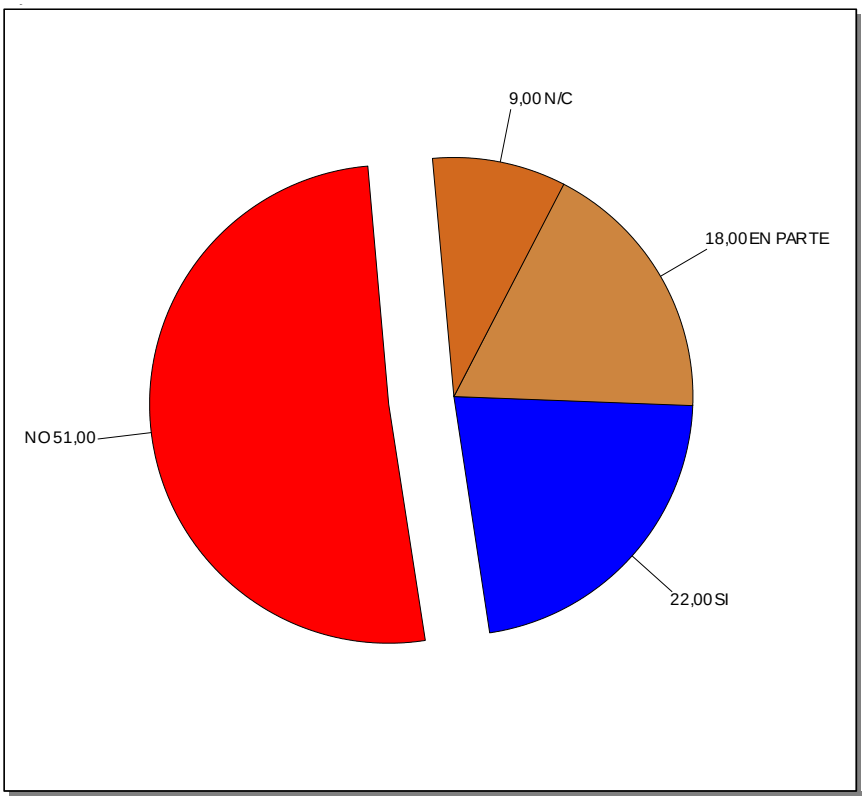


Figura 4.30 Gráfico de Resultado de Datos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 60 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 40 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben

orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

11. Organización interna de la empresa.

	P11 Organización interna de la empresa.	(1) SI	29
		(2) EN PARTE	15
		(3) NO	47
		(4) N/C	9
		Total Base sujetos (Organización)	100

Tabla 4.31 Cuadro de Resultado de Datos de una empresa
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

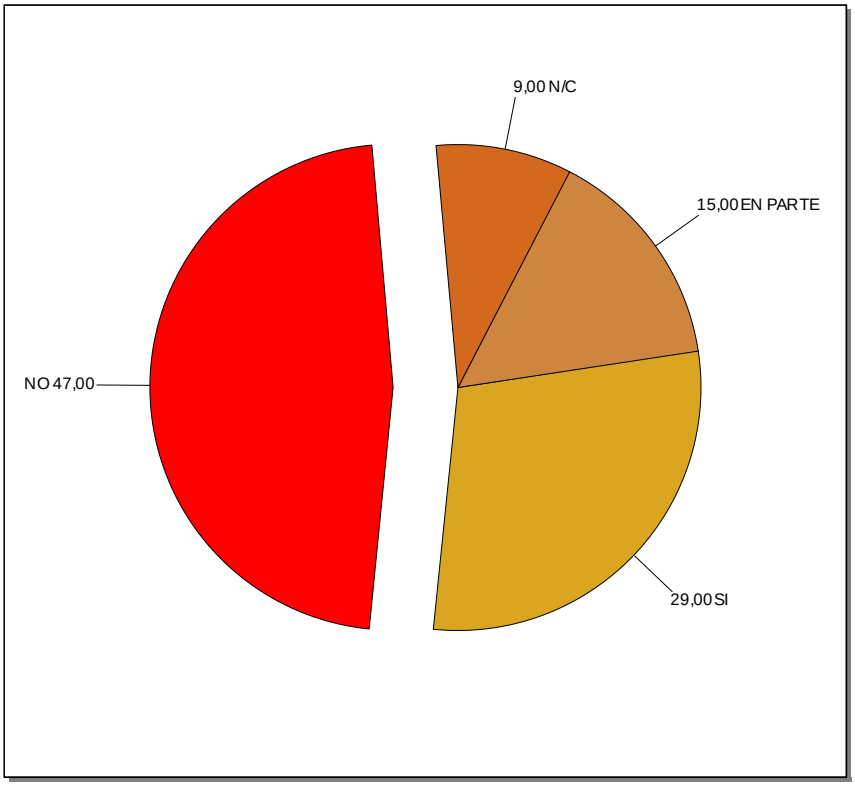


Figura 4.31 Gráfico de Resultado de Datos de una empresa
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 56 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 44 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

12. Descubrimiento y revelación de secretos.

	P12 Descubrimiento y revelación de secretos.	(1) SI	24
		(2) EN PARTE	16
		(3) NO	50
		(4) N/C	10
		Total Base sujetos (Descubrimiento)	100

Tabla 4.32 Cuadro de Descubrimiento y Revelación de secretos

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia..

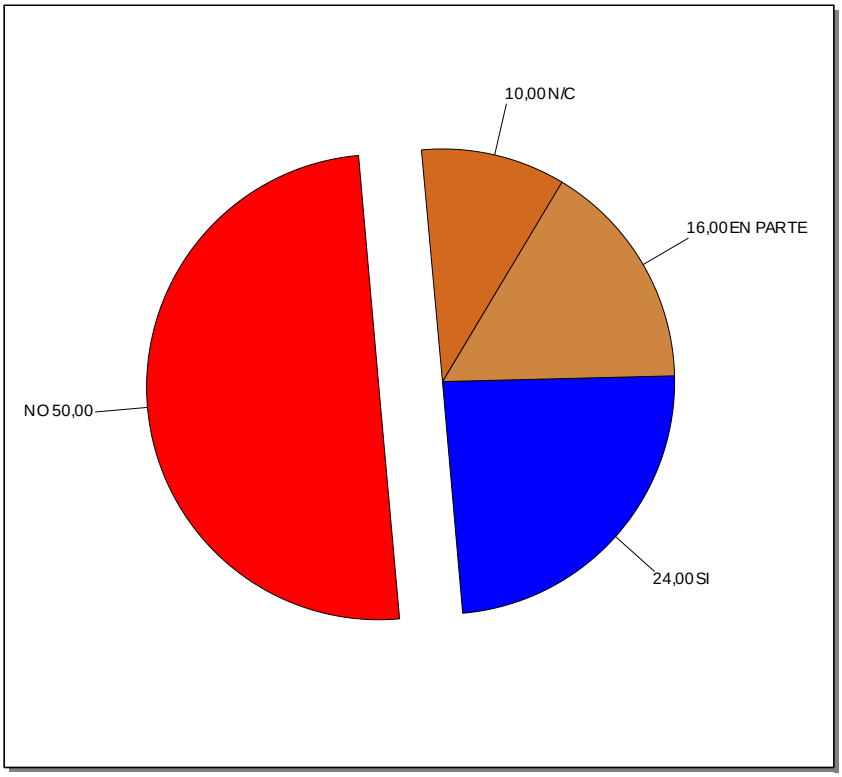


Figura 4.32 Gráfico de Descubrimiento y Revelación de secretos
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 60 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 40 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

13. Descubrimiento y revelación de secretos relativos a la defensa nacional.

	P13 Descubrimiento y revelación de secretos relativos a la defensa nacional.	(1) SI	22
		(2) EN PARTE	17
		(3) NO	52
		(4) N/C	9
		Total Base sujetos (Descubrimiento)	100

Tabla 4.33 Cuadro de Resultado de Descubrimiento y revelación de secretos relativos a la defensa nacional

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

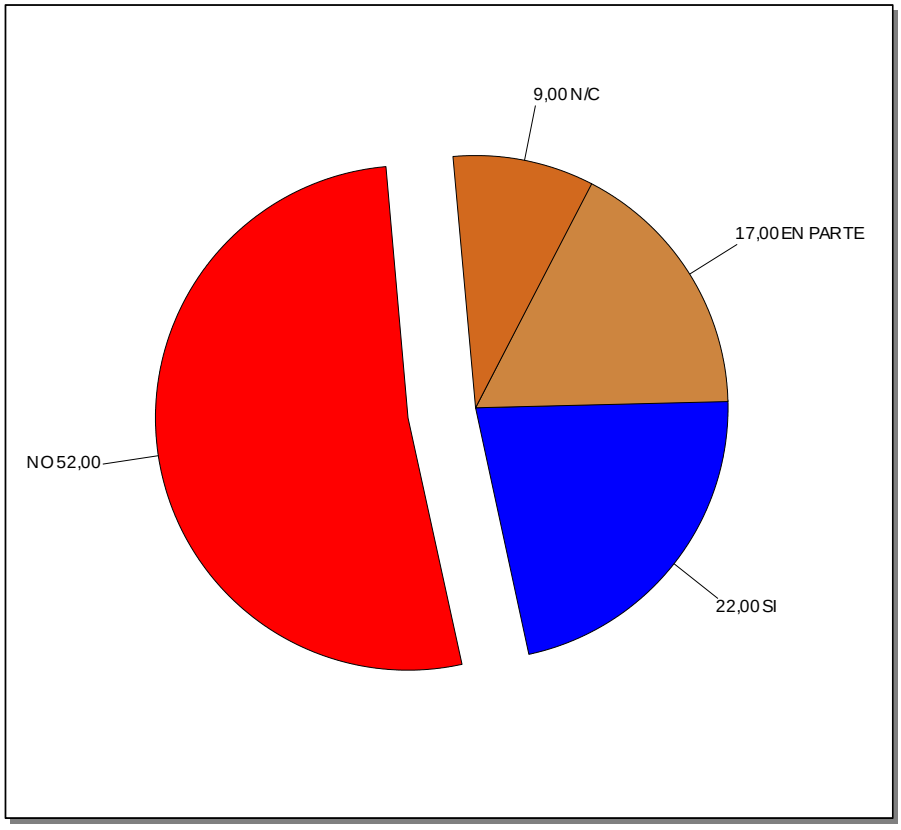


Figura 4.33 Gráfico de Resultado de Descubrimiento y revelación de secretos relativos a la defensa nacional

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 61 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la

Administración de Justicia; mientras un 39 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

14. Apoderamiento de ficheros con información de valor económico no calificable de secreto de empresa (No Tipificado).

	P14 Apoderamiento de ficheros con información de valor económico no calificable de secreto de empresa .	(1) SI	19
		(2) EN PARTE	18
		(3) NO	54
		(4) N/C	9
		Total Base sujetos (Apoderamiento de ficheros)	100

Tabla 4.34 Cuadro de Resultado de Apoderamiento de ficheros con información de valor económico

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

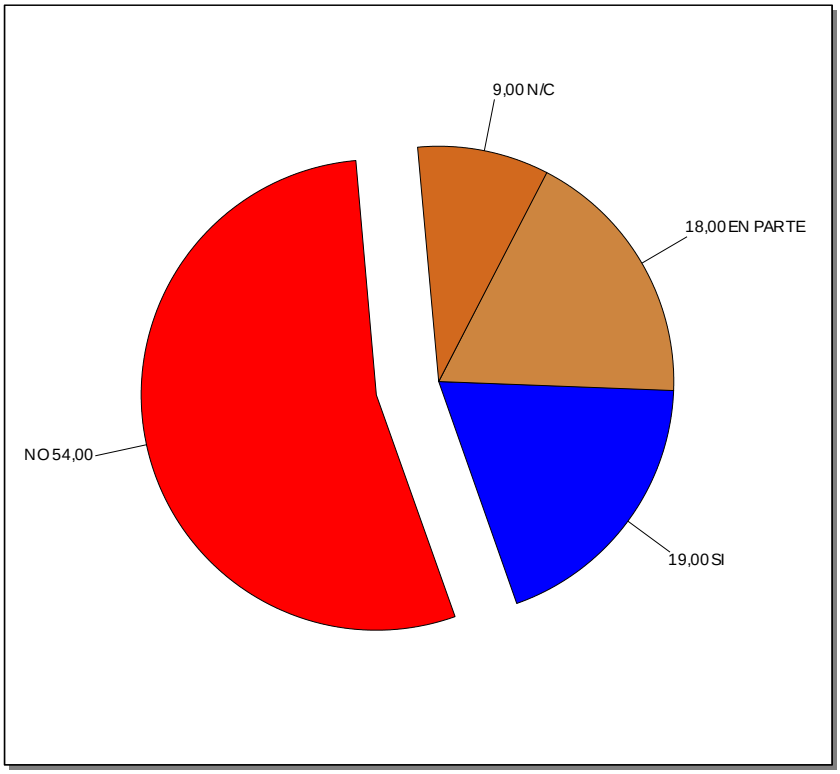


Figura 4.34 Gráfico de Resultado de Apoderamiento de ficheros con información de valor económico

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 63 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 37 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

15. Estudios generales de mercado, un listado para envíos postales, etc.

	P15 Estudios generales de mercado, un listado para envíos postales, etc.	(1) SI	23
		(2) EN PARTE	16
		(3) NO	52
		(4) N/C	9
		Total Base sujetos (Listado postales)	100

Tabla 4.35 Cuadro de Resultado de Estudios generales de mercado.
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

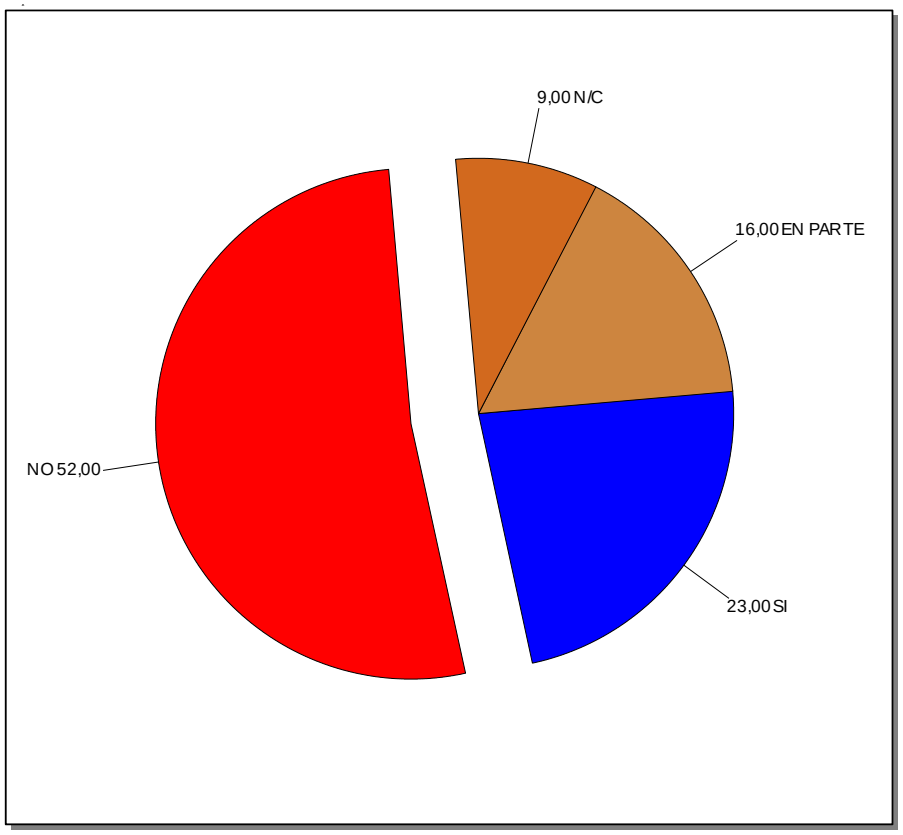


Figura 4.35 Gráfico de Resultado de Estudios generales de mercado.
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 61 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 39 % manifestaron que si tienen

conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

16. Apropiación indebida de uso.

	P16 Apropiación indebida de uso.	(1) SI	31
		(2) EN PARTE	15
		(3) NO	44
		(4) N/C	10
		Total Base sujetos (Apropiación)	100

Tabla 4.36 Cuadro de Resultado de Apropiación indebida de uso
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

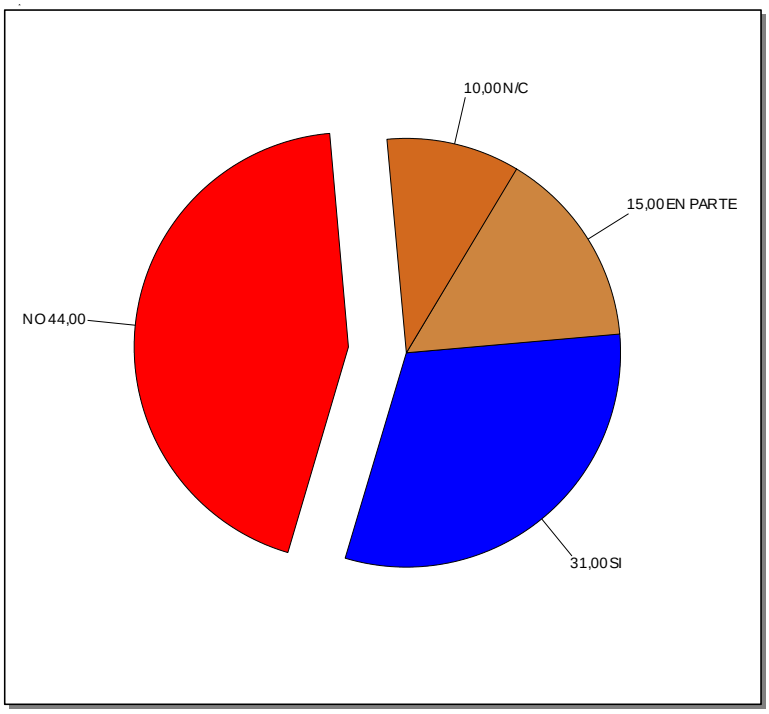


Figura 4.36 Gráfico de Resultado de Apropiación indebida de uso
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 54 % que no posee conocimientos sobre Piratería de Información o cualquier otro medio utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 46 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

17. Protección penal a los programas de ordenador y sus contenidos (piratería).

	P17 Protección penal a los programas de ordenador y sus contenidos (piratería).	(1) SI	26
		(2) EN PARTE	22
		(3) NO	44
		(4) N/C	8
		Total Base sujetos (Protección contenidos)	100

Tabla 4.37 Cuadro de Resultado de Protección penal a los programas de ordenador y sus contenidos (piratería)

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

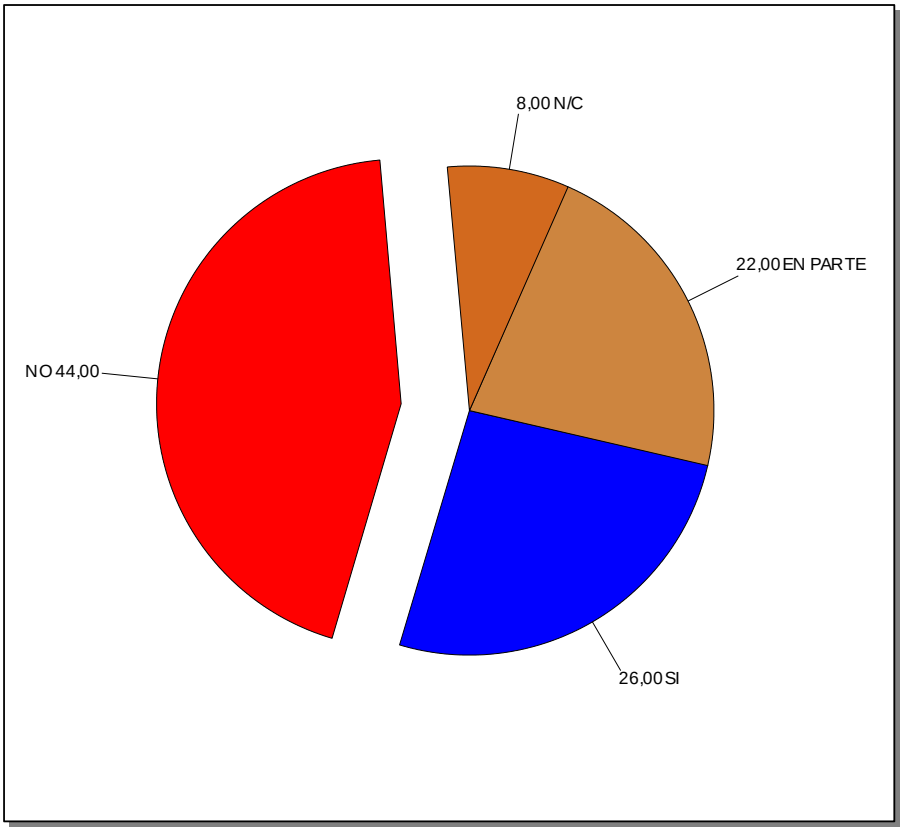


Figura 4.37 Gráfico de Resultado de Protección penal a los programas de ordenador y sus contenidos (piratería)
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 52 % que no posee conocimientos sobre Piratería de Información o cualquier otro medio utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 48 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

18. Reproducción.

	P18 Reproducción	(1) SI	43
		(2) EN PARTE	22
		(3) NO	26
		(4) N/C	9
		Total Base sujetos (Reproducción)	100

Tabla 4.38 Cuadro de Resultado de Reproducción
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

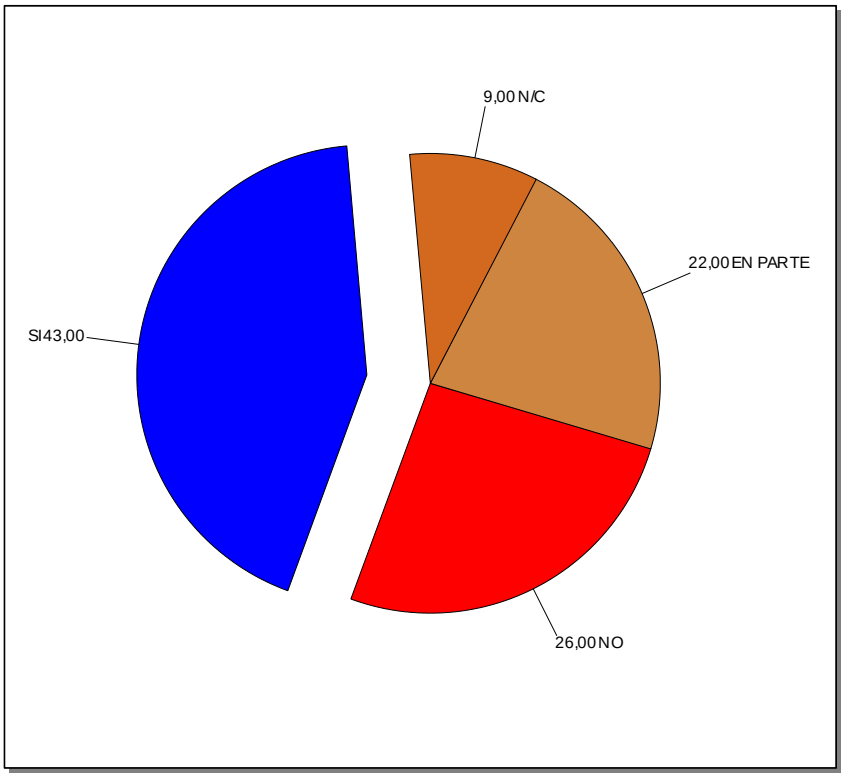


Figura 4.38 Gráfico de Resultado de Reproducción
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 35 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 65 % manifestaron que si tienen

conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

19. Plagio.

	P19 Plagio.	(1) SI	52
		(2) EN PARTE	14
		(3) NO	25
		(4) N/C	9
		Total Base sujetos (Plagio)	100

Tabla 4.39 Cuadro de Resultado de Plagio.
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

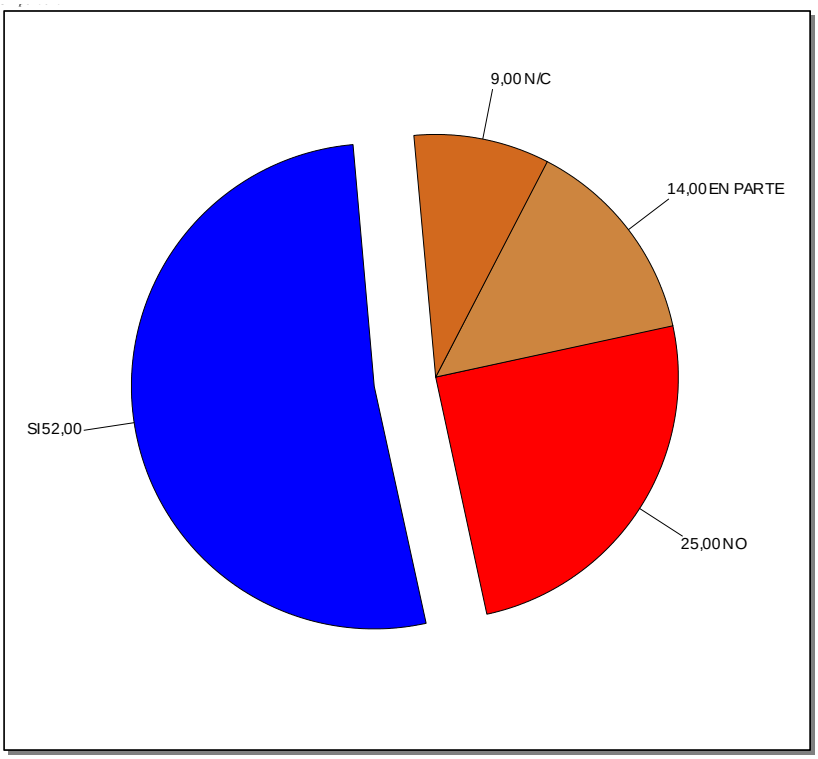


Figura 4.39 Gráfico de Resultado de Plagio.

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 34 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 66 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

20. Transformación.

	P20 Transformación	(1) SI	43
		(2) EN PARTE	18
		(3) NO	29
		(4) N/C	10
		Total Base sujetos (Transformación)	100

Tabla 4.40 Cuadro de Resultado de Transformación

Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

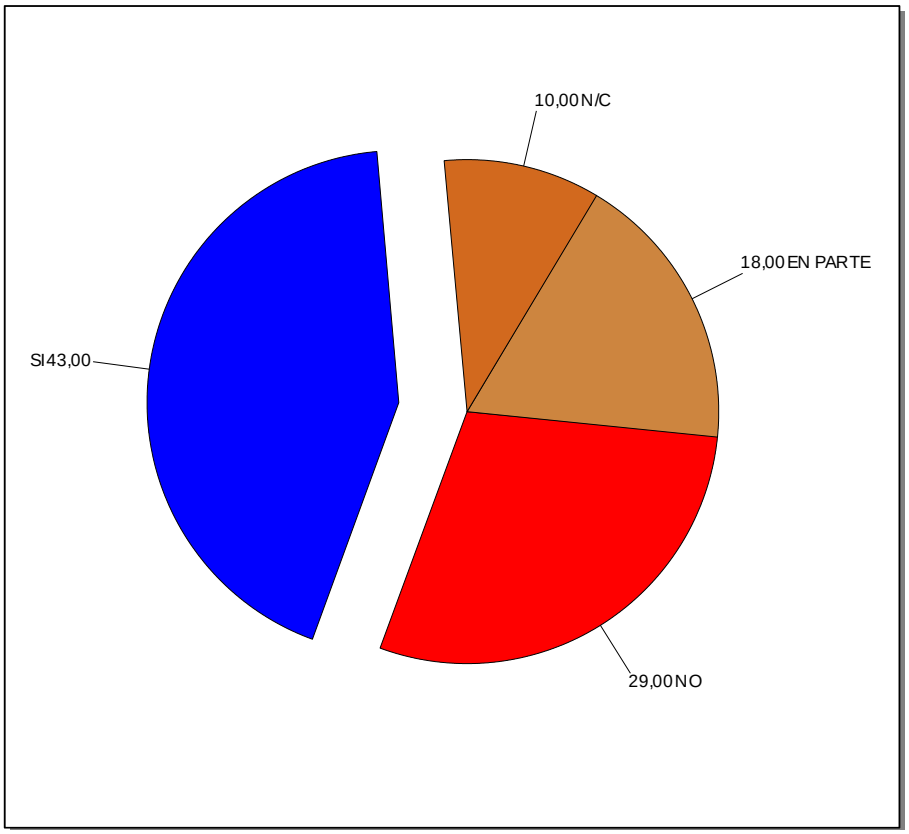


Figura 4.40 Gráfico de Resultado de Transformación
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 39 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 61 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

21. Distribución.

	P21 Distribución.	(1) SI	26
		(2) EN PARTE	21
		(3) NO	44
		(4) N/C	9
		Total Base sujetos (Distribución)	100

Tabla 4.41 Cuadro de Resultado de Distribución
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

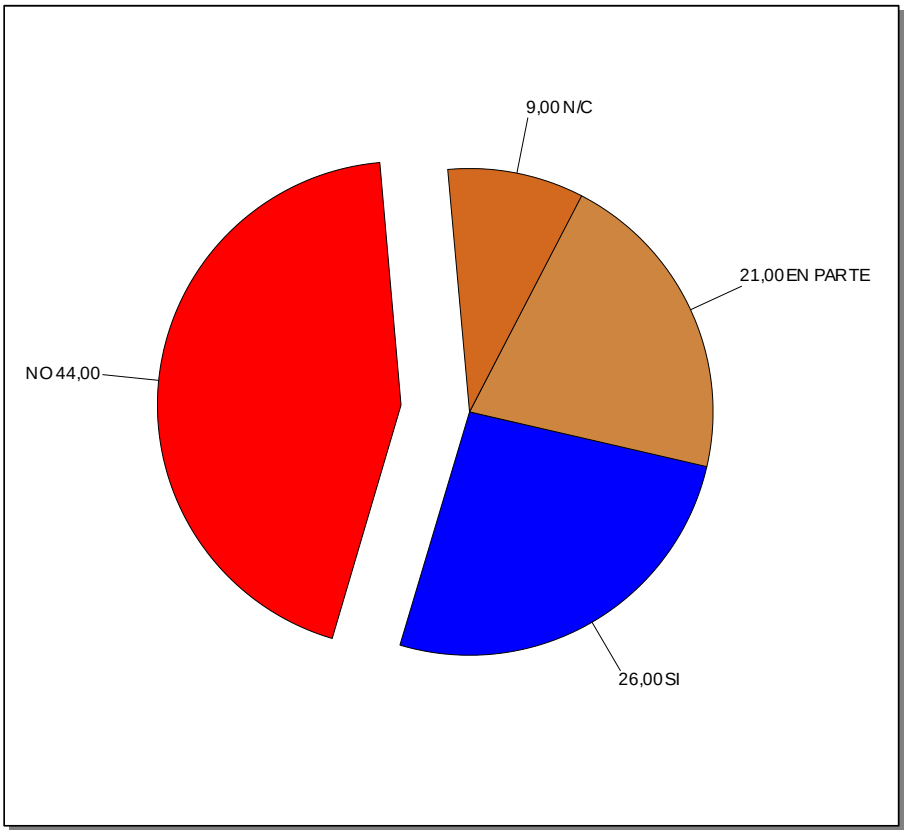


Figura 4.41 Gráfico de Resultado de Distribución
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 53 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la

Administración de Justicia; mientras un 47 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

22. Comunicación pública.

	P22 Comunicación pública.	(1) SI	45
		(2) EN PARTE	22
		(3) NO	24
		(4) N/C	9
		Total Base sujetos (Comunicación pública)	100

Tabla 4.42 Cuadro de Resultado de Comunicación publica
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

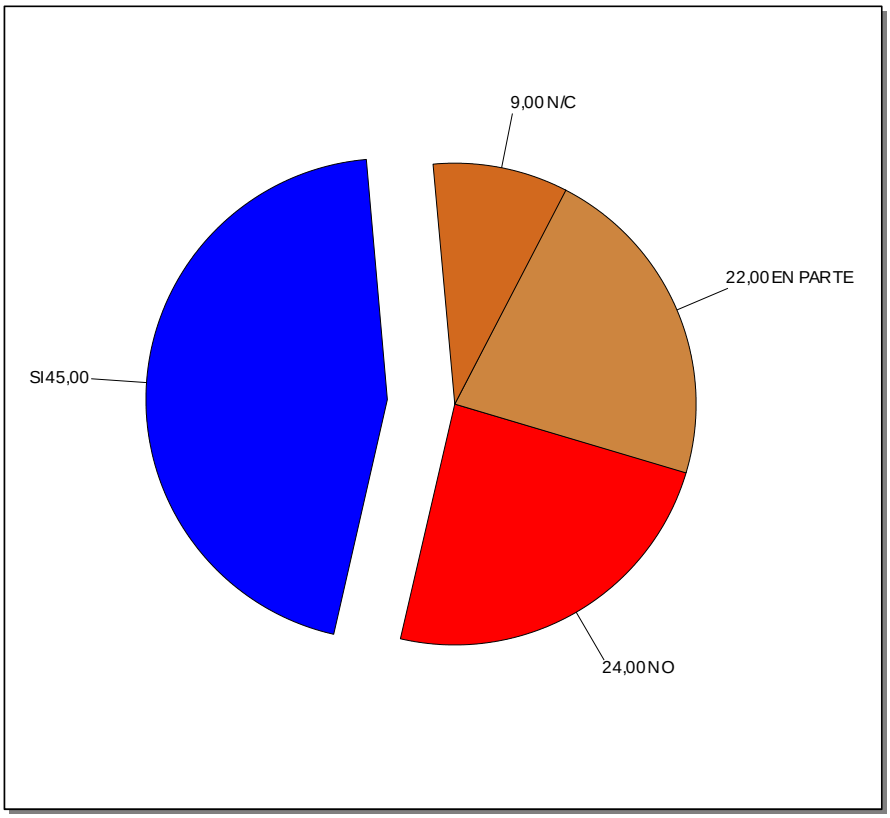


Figura 4.42 Gráfico de Resultado de Comunicación publica
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 33 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 67 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

23. Almacén de ejemplares.

	P23 Almacén de ejemplares.	(1) SI	43
		(2) EN PARTE	18
		(3) NO	29
		(4) N/C	10
		Total Base sujetos (Almacén ejemplares)	100

Tabla 4.43 Cuadro de Resultado de Almacén de ejemplares
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

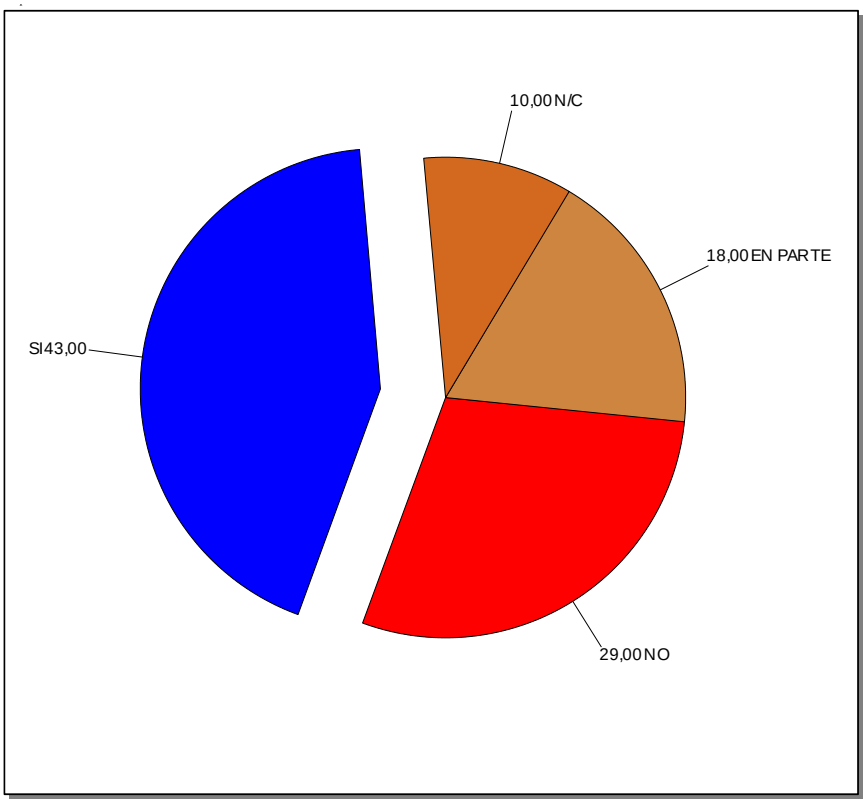


Figura 4.43 Gráfico de Resultado de Almacén de ejemplares
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 39 % que no posee conocimientos sobre el Robo de Información utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 61 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben

orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

24. Utilización ilegítima de terminales de comunicaciones (defraudaciones de telecomunicaciones) (No Tipificado).

	P24 Utilización ilegítima de terminales de comunicaciones (defraudaciones de telecomunicaciones) (No Tipificado).	(1) SI	26
		(2) EN PARTE	20
		(3) NO	45
		(4) N/C	9
		Total Base sujetos (Telecomunicaciones)	100

Tabla 4.44 Cuadro de Resultado de Utilización ilegítima de terminales de comunicaciones
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

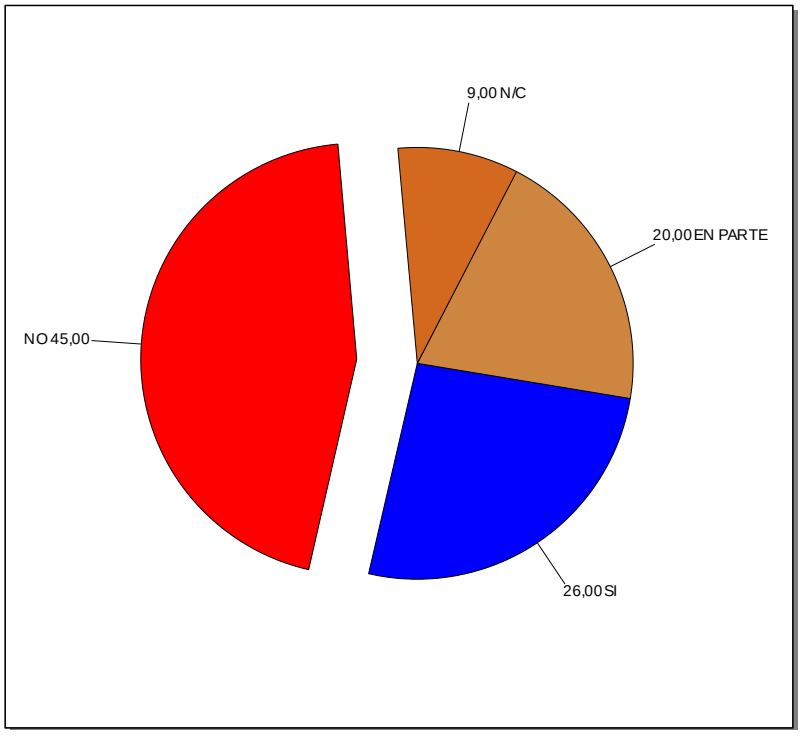


Figura 4.44 Gráfico de Resultado de Utilización ilegítima de terminales de comunicaciones
Fuente: Datos Tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. De las personas encuestadas indicaron un 54 % que no posee conocimientos sobre Piratería de Información o cualquier otro medio utilizando las TICS y que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 46 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

RESULTADOS FORMULARIO 3 (F3): Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

DELITOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS

1. **Estafa perpetrada a través de medios informáticos.**

	P1 Estafa perpetrada a través de medios informáticos.	(1) SI	57
		(2) EN PARTE	22
		(3) NO	12
		(4) N/C	9
		Total Base sujetos (Informáticos)	100

Tabla 4.45 Cuadro de Resultado de Delitos Cometidos A Través De Sistemas Informáticos
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

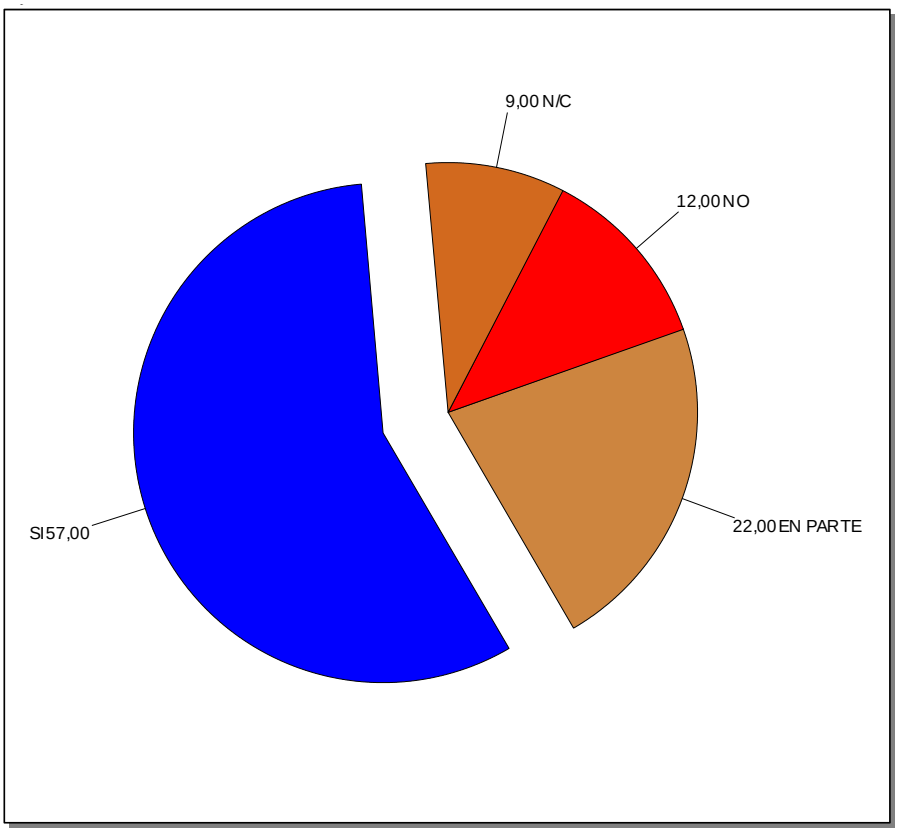


Figura 4.45 Gráfico de Resultado de Delitos Cometidos A Través De Sistemas Informáticos
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 79 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

2. Apoderamiento de Dinero utilizando tarjetas de cajeros automáticos.

	P2 Apoderamiento de dinero utilizando tarjetas de cajeros automáticos	(1) SI	60
		(2) EN PARTE	20
		(3) NO	15
		(4) N/C	5
		Total Base sujetos (Apoderamiento de dinero)	100

Tabla 4.46 Cuadro de Resultado de Apoderamiento de Dinero utilizando tarjetas de cajeros automáticos.
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

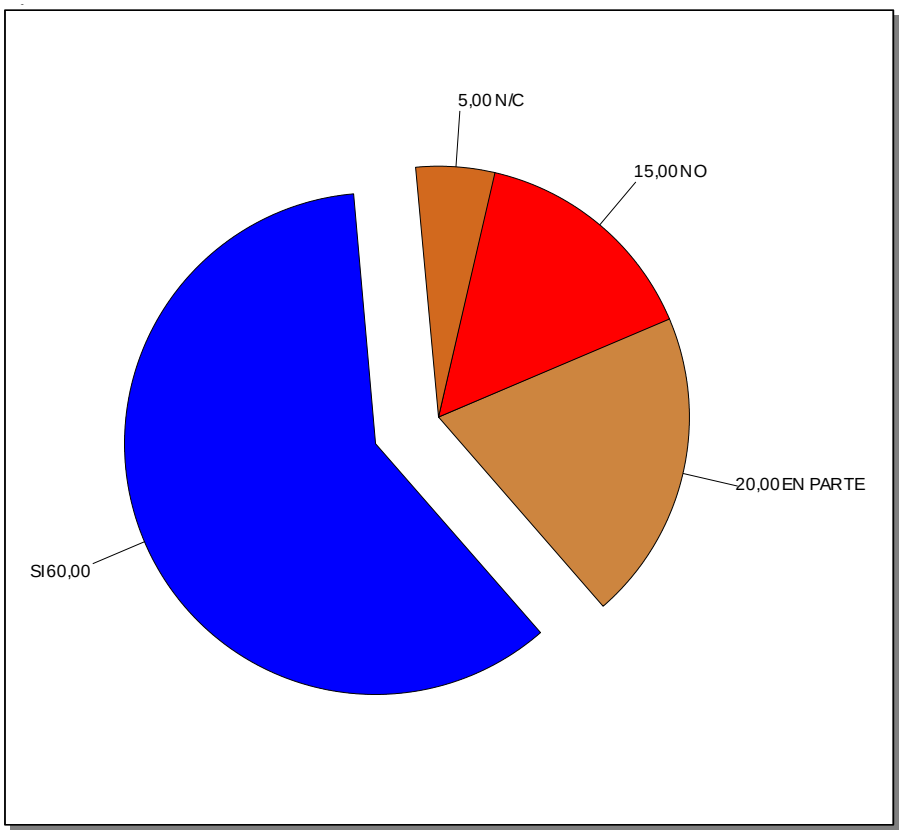


Figura 4.46 Gráfico de Resultado de Apoderamiento de Dinero utilizando tarjetas de cajeros automáticos.
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 20 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 80 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

Utilización del correo electrónico con finalidad criminal (No Tipificado).

3. **Amenazas.**

	P3 Amenazas.	(1) SI	61
		(2) EN PARTE	21
		(3) NO	14
		(4) N/C	4
		Total Base sujetos (Amenazas)	100

Tabla 4.47 Cuadro de Resultado de Amenazas
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

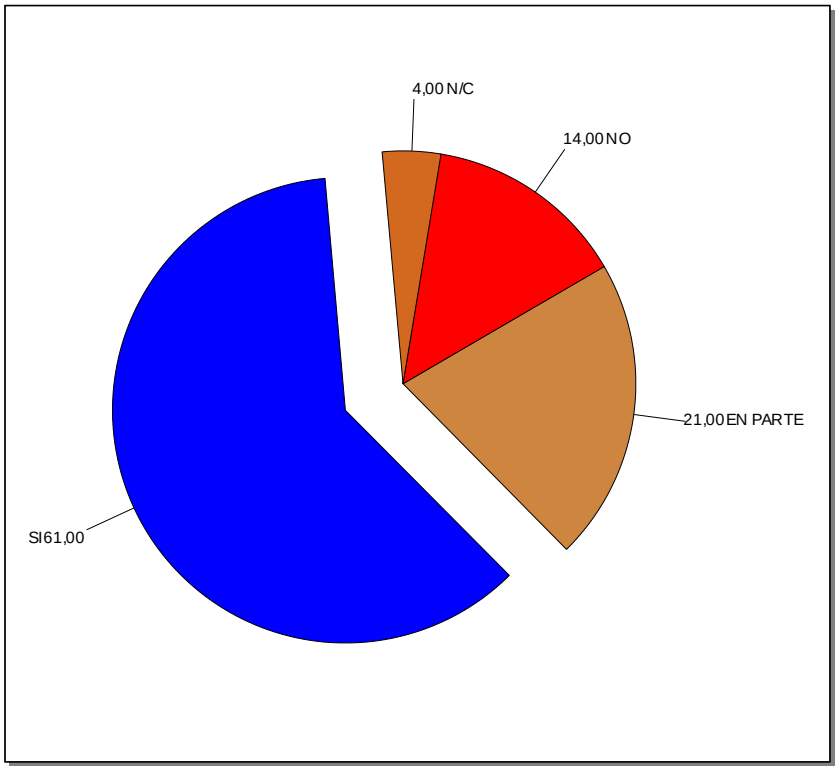


Figura 4.47 Gráfico de Resultado de Amenazas
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 18 % que no posee

conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 82 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

4. Injurias.

	P4 Injurias.	(1) SI	64
		(2) EN PARTE	15
		(3) NO	12
		(4) N/C	9
		Total Base sujetos (Injurias)	100

Tabla 4.48 Cuadro de Resultado de Injurias
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

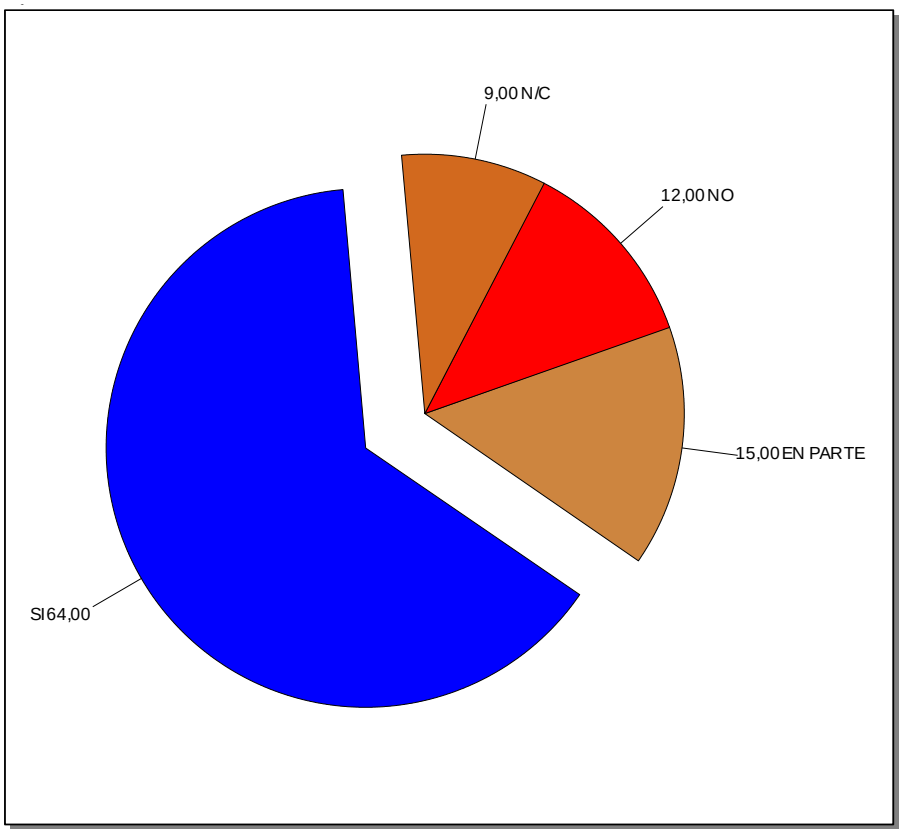


Figura 4.48 Gráfico de Resultado de Injurias
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 79 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

5. Inducción al delito.

	P5 Inducción al delito.	(1) SI	62
		(2) EN PARTE	17
		(3) NO	12
		(4) N/C	9
		Total Base sujetos (Inducción delito)	100

Tabla 4.49 Cuadro de Resultado de Inducción al delito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

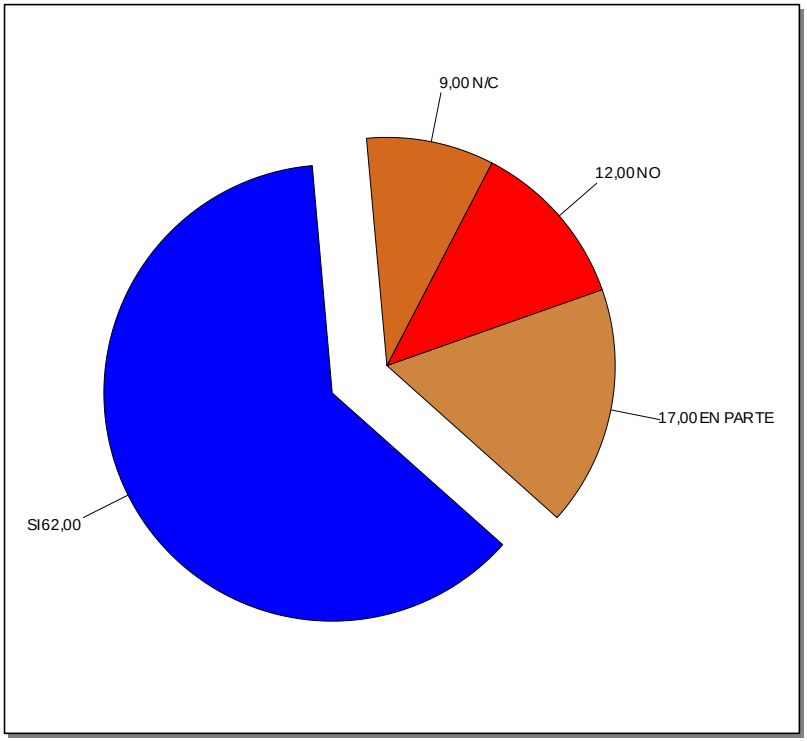


Figura 4.49 Gráfico de Resultado de Inducción al delito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 79 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los

Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

6. Actos preparatorios y de cooperación para el delito.

	P6 Actos preparatorios y de cooperación para el delito.	(1) SI	48
		(2) EN PARTE	28
		(3) NO	18
		(4) N/C	6
		Total Base sujetos (Preparatorios)	100

Tabla 4.50 Cuadro de Resultado de Actos preparatorios y de cooperación para el delito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

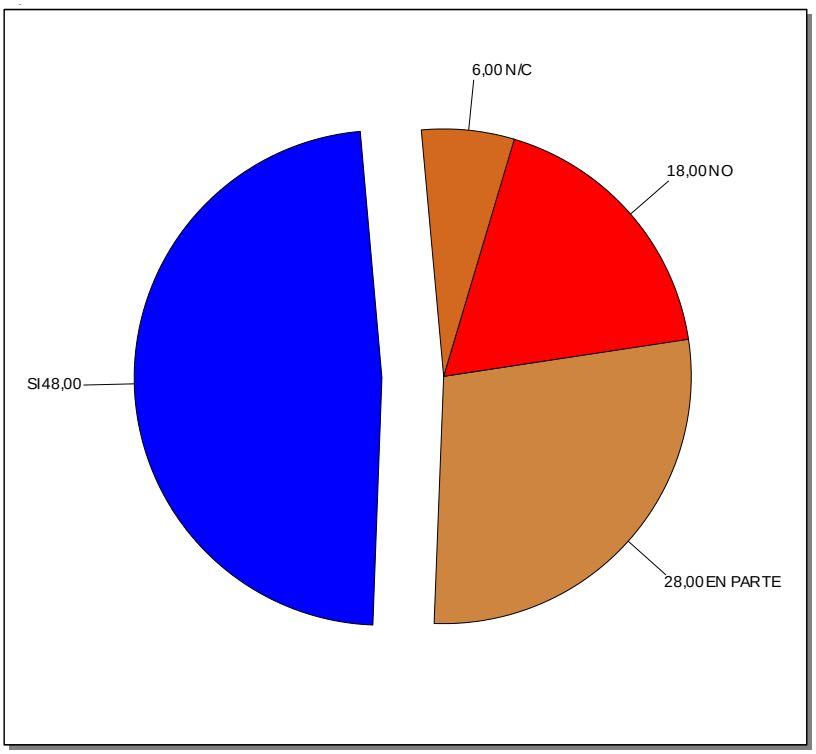


Figura 4.50 Gráfico de Resultado de Actos preparatorios y de cooperación para el delito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 24 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la

finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 76 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

7. Actividades de extorsión.

	P7 Actividades de extorsión	(1) SI	57
		(2) EN PARTE	21
		(3) NO	17
		(4) N/C	5
		Total Base sujetos (Actividades extorsión)	100

Tabla 4.51 Cuadro de Resultado de Actividades de extorsión
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

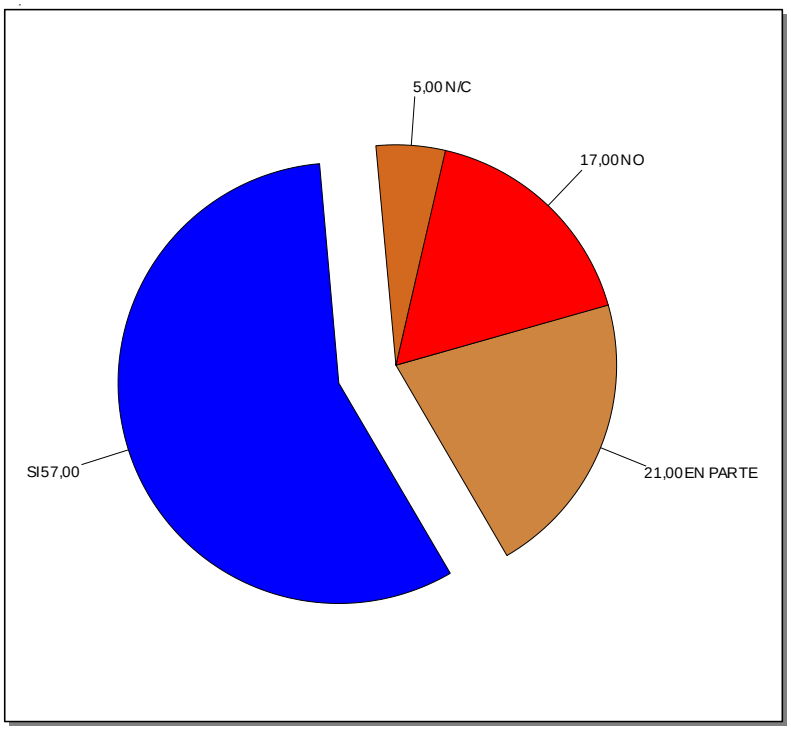


Figura 4.51 Gráfico de Resultado de Actividades de extorsión
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 22 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 78 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

8. Utilización de Internet como medio criminal (No Tipificado).

	P8 Utilización de internet como medio criminal .	(1) SI	24
		(2) EN PARTE	54
		(3) NO	17
		(4) N/C	5
		Total Base sujetos (Utilización de internet)	100

Tabla 4.52 Cuadro de Resultado de Utilización de Internet como medio criminal
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

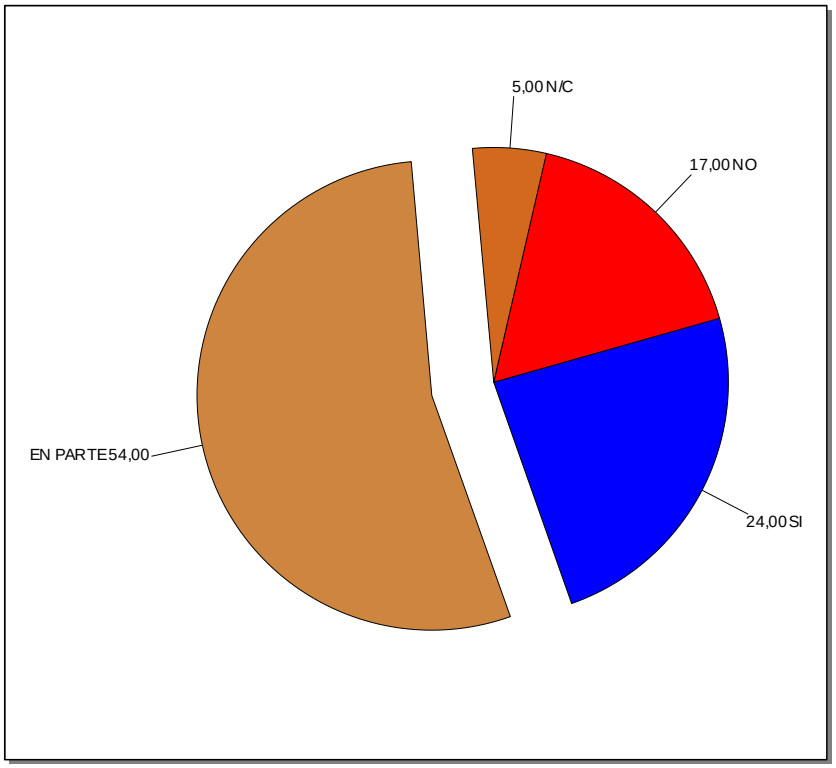


Figura 4.52 Gráfico de Resultado de Utilización de Internet como medio criminal
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 22 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 78 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

9. Difusión de contenidos o material ilícito.

	P9 Difusión de contenidos o material ilícito.	(1) SI	56
		(2) EN PARTE	23
		(3) NO	12
		(4) N/C	9
		Total Base sujetos (Contenidos o material)	100

Tabla 4.53 Cuadro de Resultado de Difusión de contenidos o material ilícito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

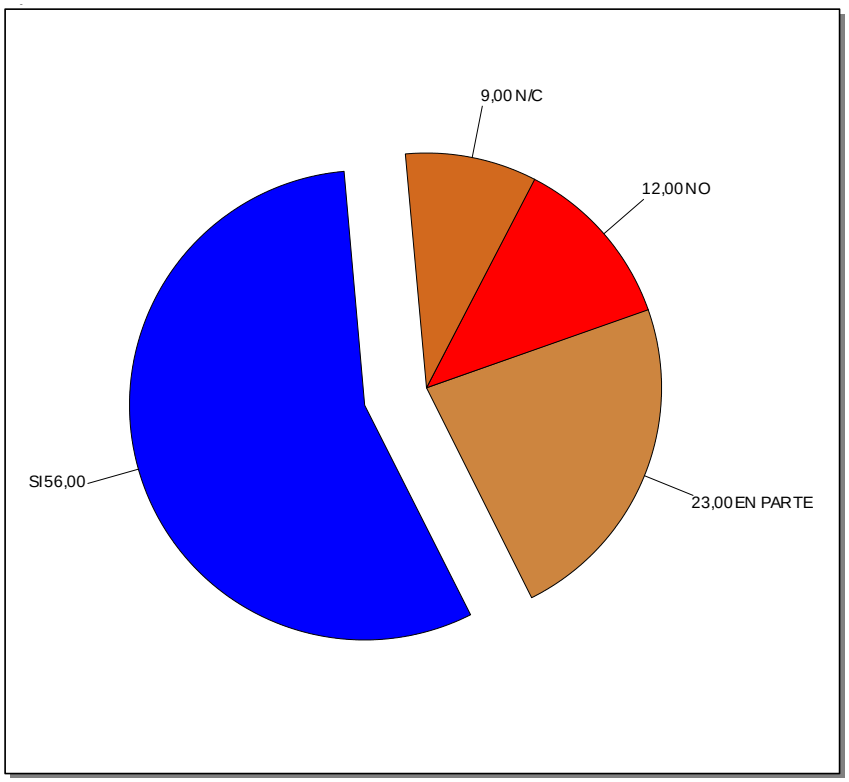


Figura 4.53 Gráfico de Resultado de Difusión de contenidos o material ilícito
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 79 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los

Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

10. Material pornográfico: difusión, posesión.

	P10 Material pornográfico: difusión, posesión.	(1) SI	59
		(2) EN PARTE	24
		(3) NO	12
		(4) N/C	5
		Total Base sujetos (Pornográfico)	100

Tabla 4.54 Cuadro de Resultado de Material pornográfico: difusión, posesión
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

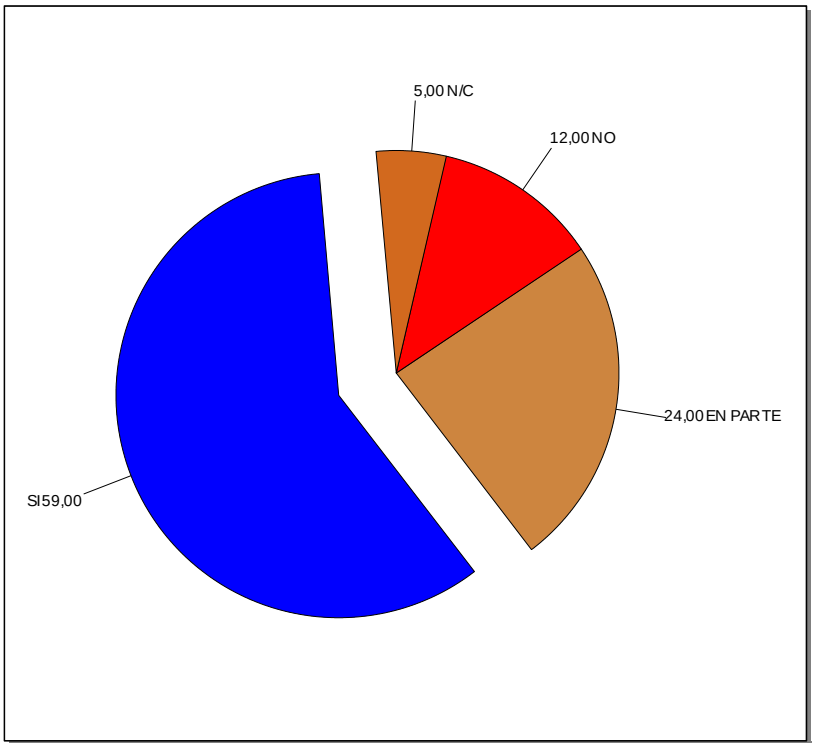


Figura 4.54 Gráfico de Resultado de Material pornográfico: difusión, posesión
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 17 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación

de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 83 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

11. Incitación al odio o a la discriminación.

	P11 Incitación al odio o a la discriminación.	(1) SI	54
		(2) EN PARTE	26
		(3) NO	15
		(4) N/C	5
		Total Base sujetos (Discriminación)	100

Tabla 4.55 Cuadro de Resultado de Incitación al odio o a la discriminación
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

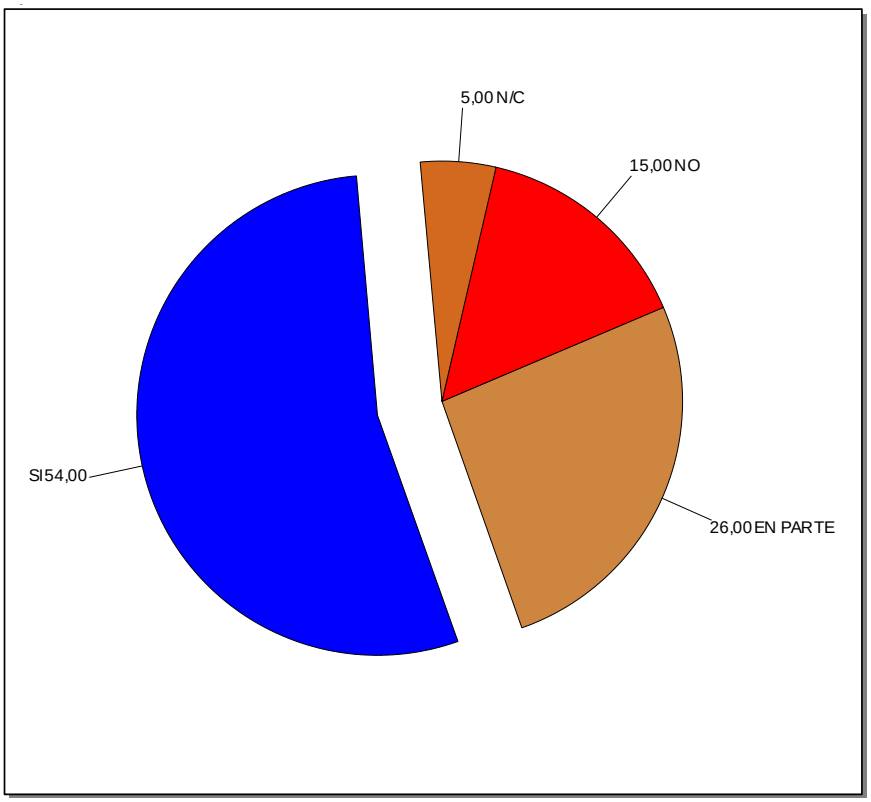


Figura 4.55 Gráfico de Resultado de Incitación al odio o a la discriminación
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 20 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 80 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

12. Piratería (Instrumento Físico).

	P12 Piratería (Instrumento Físico).	(1) SI	62
		(2) EN PARTE	22
		(3) NO	7
		(4) N/C	9
		Total Base sujetos (Piratería)	100

Tabla 4.56 Cuadro de Resultado de Piratería
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

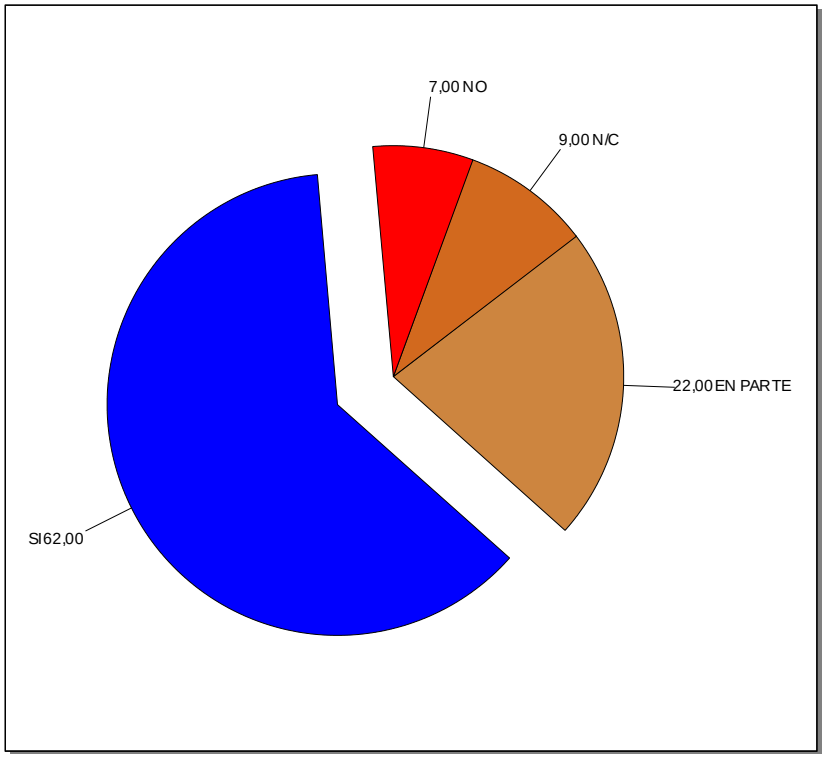


Figura 4.56 Gráfico de Resultado de Piratería
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 16 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 84 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

13. Internet (Instrumento Virtual).

	P13 Internet (Instrumento Virtual).	(1) SI	64
		(2) EN PARTE	17
		(3) NO	10
		(4) N/C	9
		Total Base sujetos (Internet)	100

Tabla 4.57 Cuadro de Resultado de Internet
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

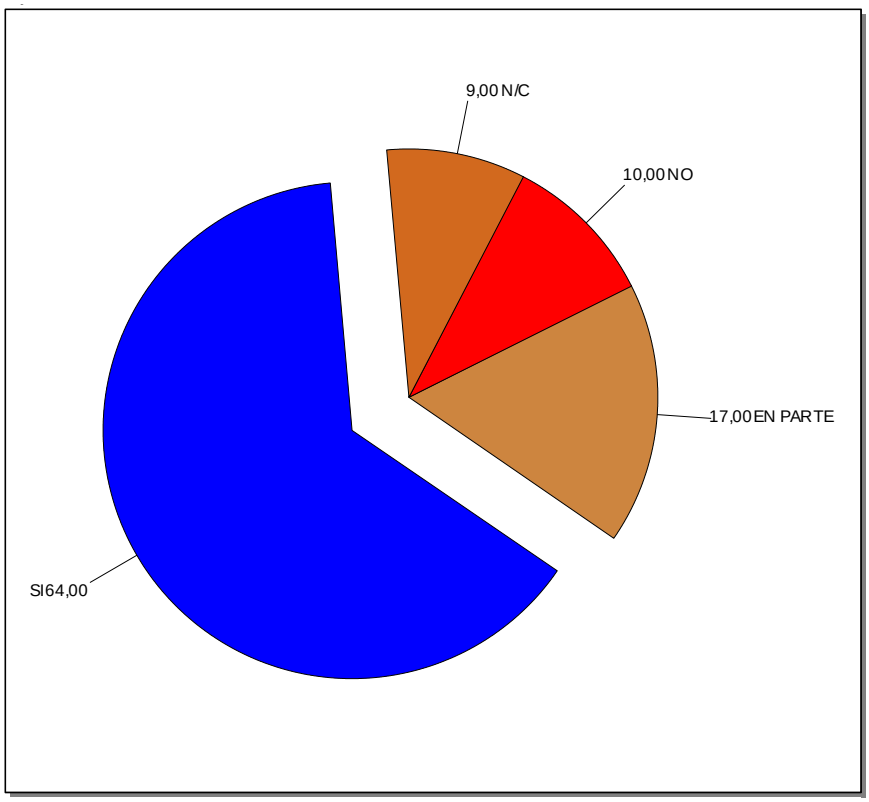


Figura 4.57 Gráfico de Resultado de Internet
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 19 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 81 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los

Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

14. Robo de Identidad – Phishing.

	P14 Robo de identidad – phishing.	(1) SI	48
		(2) EN PARTE	30
		(3) NO	15
		(4) N/C	7
		Total Base sujetos (Identidad)	100

Tabla 4.58 Cuadro de Resultado de Robo de Identidad
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

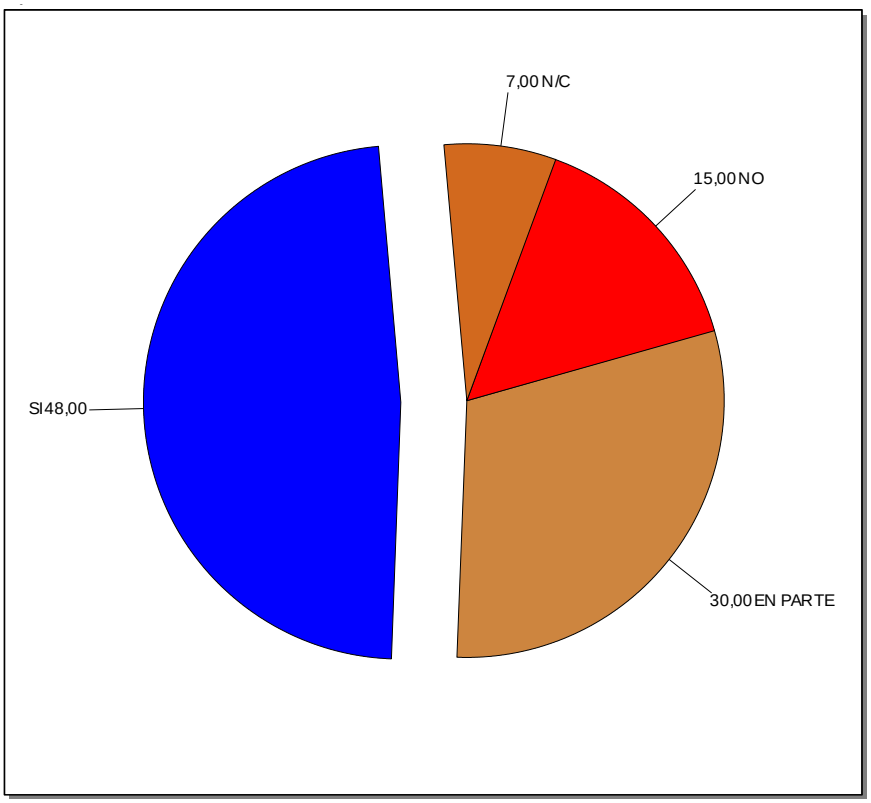


Figura 4.58 Gráfico de Resultado de Robo de Identidad
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 22 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación

de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 78 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

15. Spam.

	P15 Spam	(1) SI	25
		(2) EN PARTE	20
		(3) NO	49
		(4) N/C	6
		Total Base sujetos (Spam)	100

Tabla 4.59 Cuadro de Resultado de Spam
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

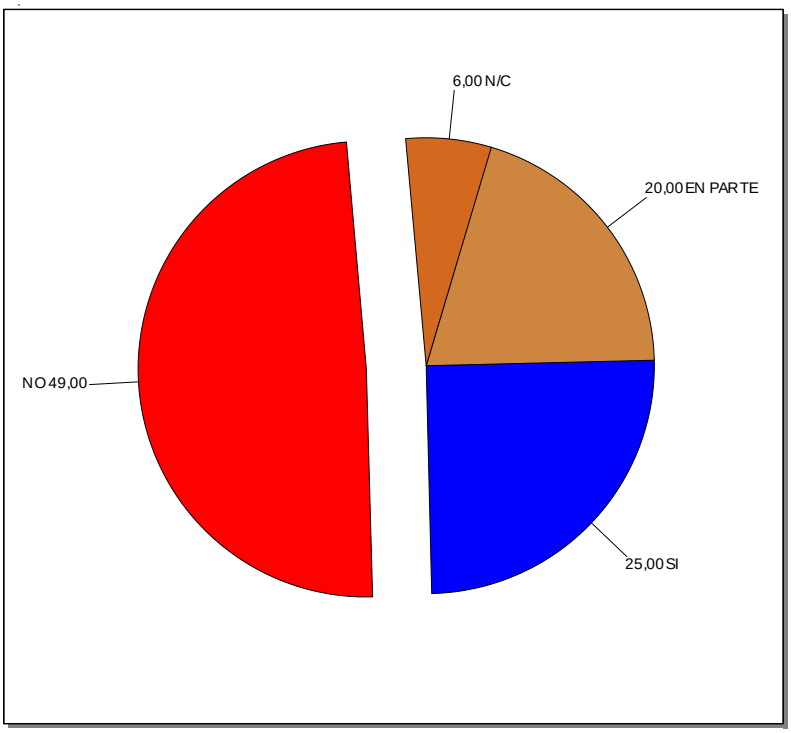


Figura 4.59 Gráfico de Resultado de Spam
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 55 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 45 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

16. Virus.

	P16 Virus	(1) SI	61
		(2) EN PARTE	18
		(3) NO	12
		(4) N/C	9
		Total Base sujetos (Virus)	100

Tabla 4.60 Cuadro de Resultado de Virus
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

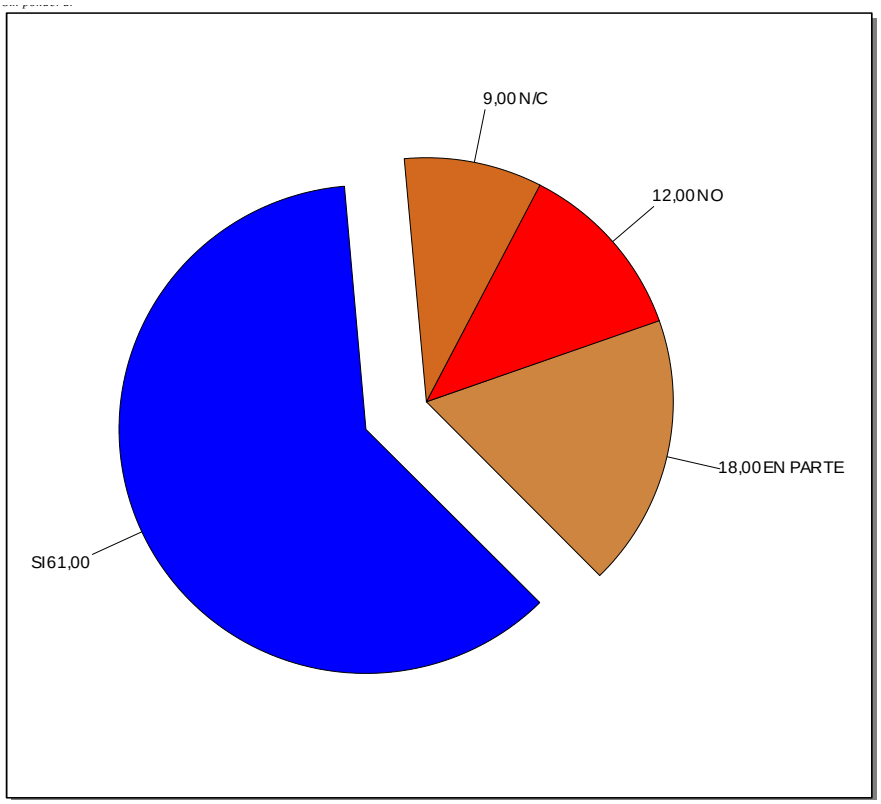


Figura 4.60 Gráfico de Resultado de Virus
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 79 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

17. Uso comercial no ético – Cybertorts.

	P17 Uso comercial no ético – cybertorts.	(1) SI	27
		(2) EN PARTE	20
		(3) NO	41
		(4) N/C	12
		Total Base sujetos (Comercial cybertorts)	100

Tabla 4.61 Cuadro de Resultado de Uso comercial no ético – Cybertorts
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

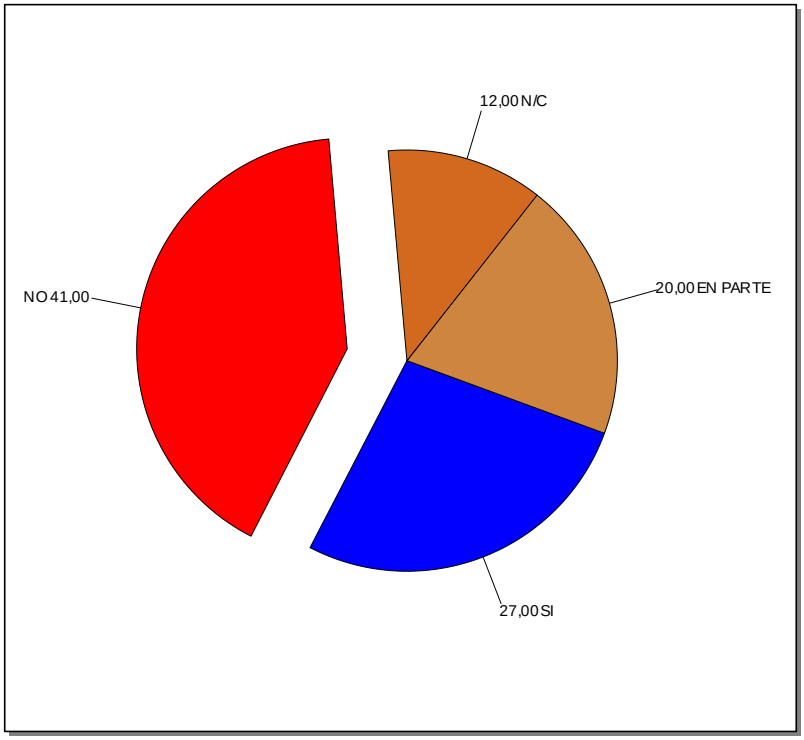


Figura 4.61 Gráfico de Resultado de Uso comercial no ético – Cybertorts
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 53 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 47 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas

tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

Utilización de Equipos de Telecomunicaciones como medio criminal (No Tipificado).

18. Redes.

	P18 Redes	(1) SI	26
		(2) EN PARTE	21
		(3) NO	44
		(4) N/C	9
		Total Base sujetos (Redes)	100

Tabla 4.62 Cuadro de Resultado de Redes
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

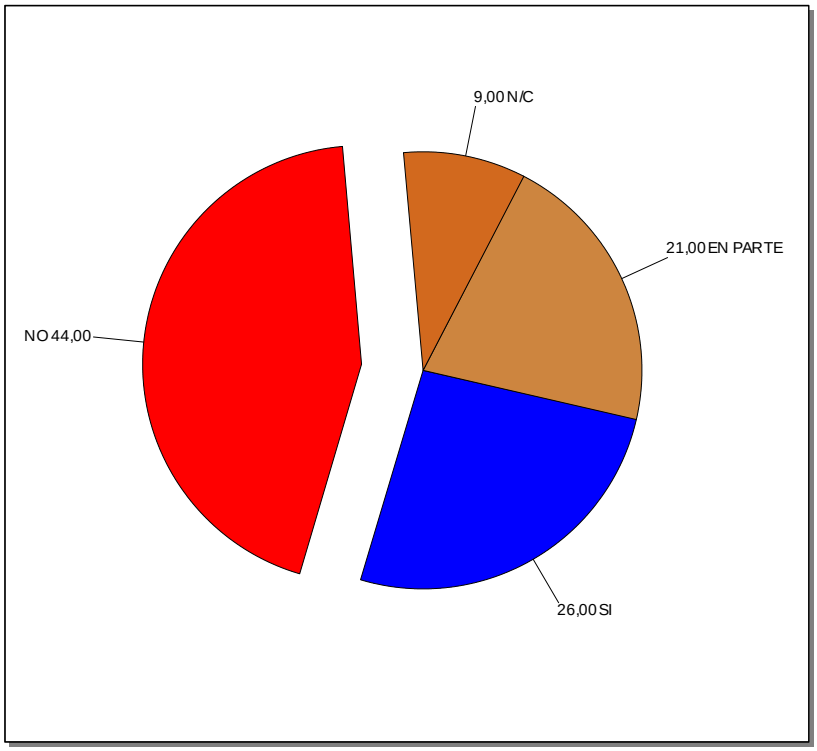


Figura 4.62 Gráfico de Resultado de Redes
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 53 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación

de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 47 % manifestaron que si tienen conocimiento sobre esta temática. Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

19. TV x IP.

	P19 Tv x ip.	(1) SI	17
		(2) EN PARTE	24
		(3) NO	51
		(4) N/C	8
		Total Base sujetos (Tv ip)	100

Tabla 4.63 Cuadro de Resultado de TV x IP
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

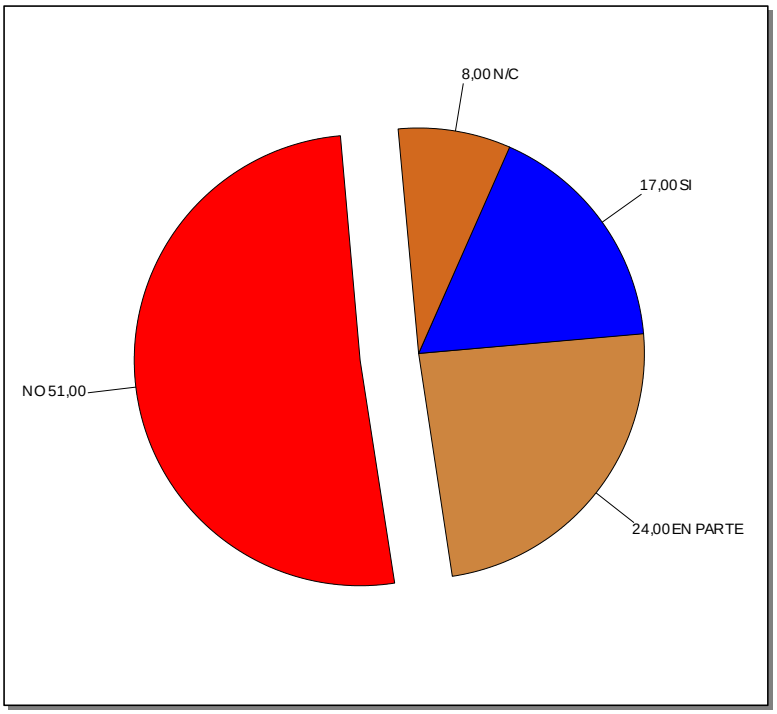


Figura 4.63 Gráfico de Resultado de TV x IP
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 59 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 41 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

20. Voz x IP (Telefonía IP).

	P20 Voz x IP (Telefonia IP).	(1) SI	27
		(2) EN PARTE	17
		(3) NO	44
		(4) N/C	12
		Total Base sujetos (Ip voz)	100

Tabla 4.64 Cuadro de Resultado de Voz x IP (Telefonía IP)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

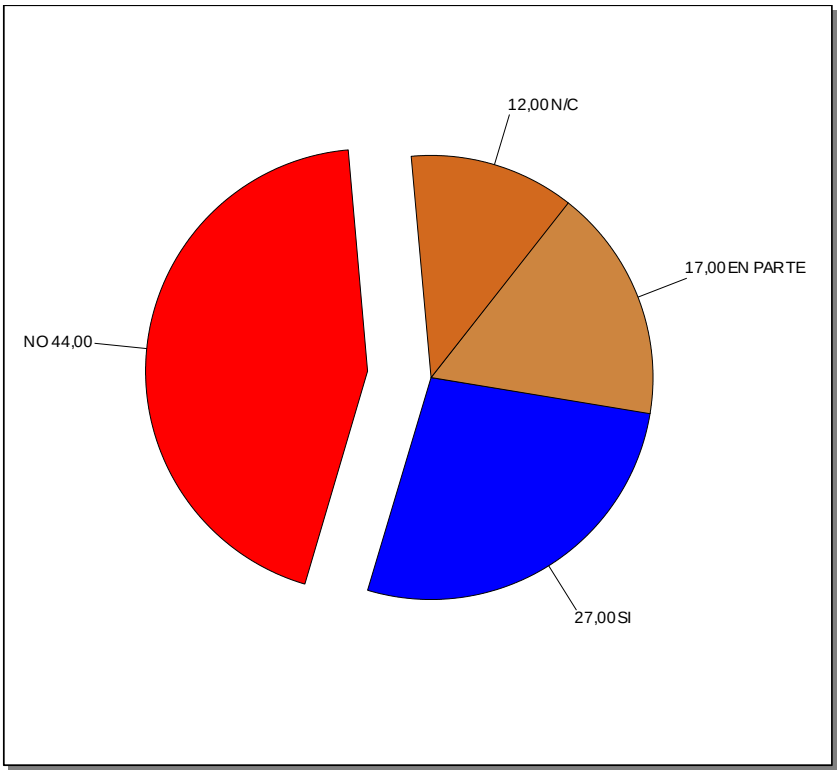


Figura 4.64 Gráfico de Resultado de Voz x IP (Telefonía IP)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 56 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 44 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

21. Internet.

	P21 Internet	(1) SI	64
		(2) EN PARTE	17
		(3) NO	11
		(4) N/C	8
		Total Base sujetos (Internet)	100

Tabla 4.65 Cuadro de Resultado de Internet
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

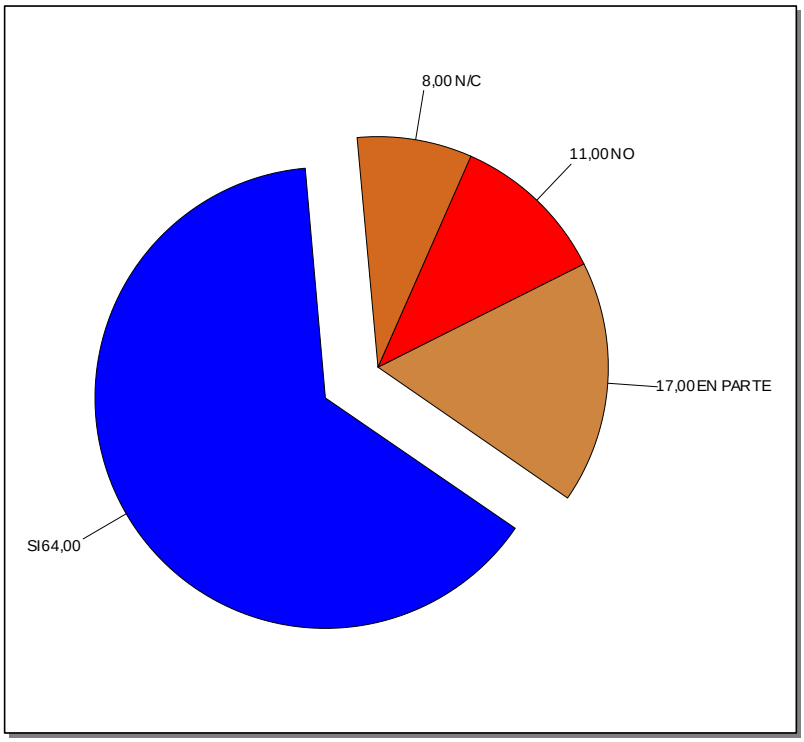


Figura 4.65 Gráfico de Resultado de Internet
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 19 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 81 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla

curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

22. Telefonía Celular.

	P22 Telefonía celular	(1) SI	64
		(2) EN PARTE	21
		(3) NO	12
		(4) N/C	3
		Total Base sujetos (Telefonía celular)	100

Tabla 4.66 Cuadro de Resultado de Telefonía Celular
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

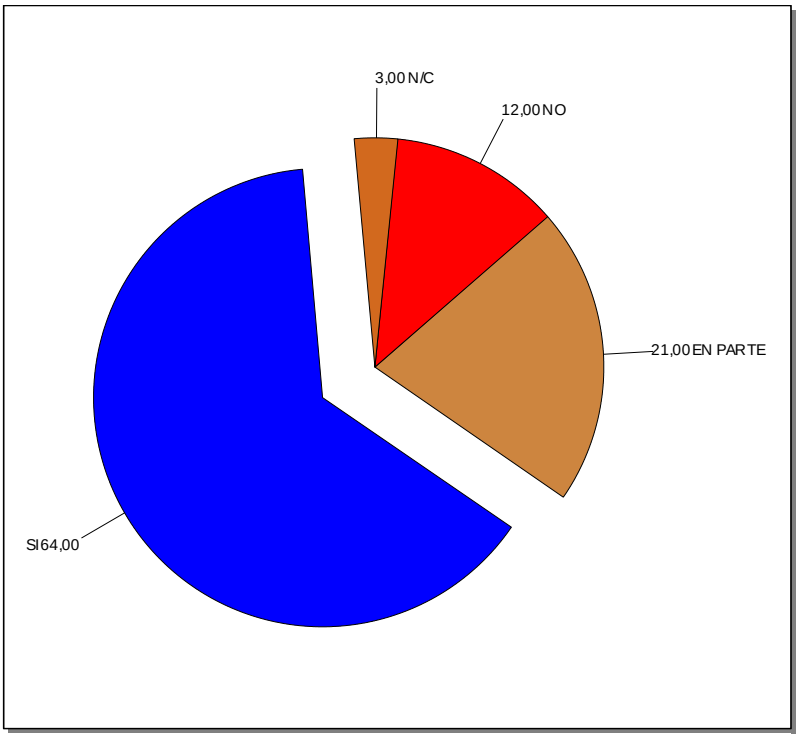


Figura 4.66 Gráfico de Resultado de Telefonía Celular
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 15 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación

de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 85 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

23. Smartphone (BlackBerry y teléfonos inteligentes, PDA).

	P23 Smartphone (Blackberrys y teléfonos inteligentes, PDA).	(1) SI	35
		(2) EN PARTE	26
		(3) NO	29
		(4) N/C	10
		Total Base sujetos (Smartphone)	100

Tabla 4.67 Cuadro de Resultado de Smartphone (Blackberrys y teléfonos inteligentes, PDA)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

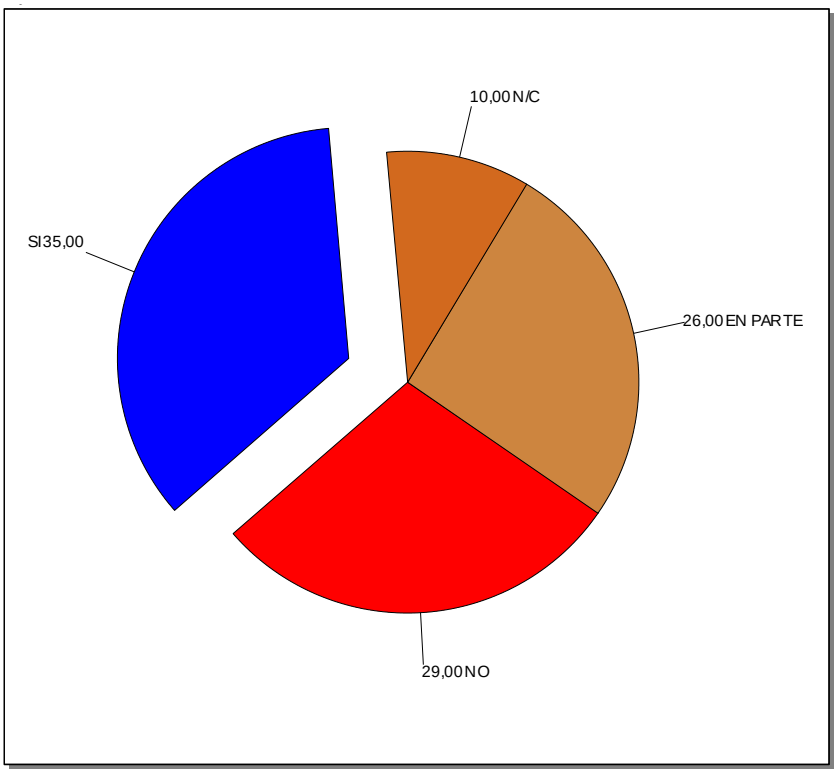


Figura 4.67 Gráfico de Resultado de Smartphone (Blackberrys y teléfonos inteligentes, PDA)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 39 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 61 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

24. Servicios inalámbricos (Bluetooth, WIFI, WIMAX).

	P24 Servicios inalámbricos (Bluetooth, WIFI, WIMAX).	(1) SI	55
		(2) EN PARTE	23
		(3) NO	14
		(4) N/C	8
		Total Base sujetos (Servicios inalámbricos)	100

Tabla 4.68 Cuadro de Resultado de Servicios inalámbricos (Bluetooth, WIFI, WIMAX)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

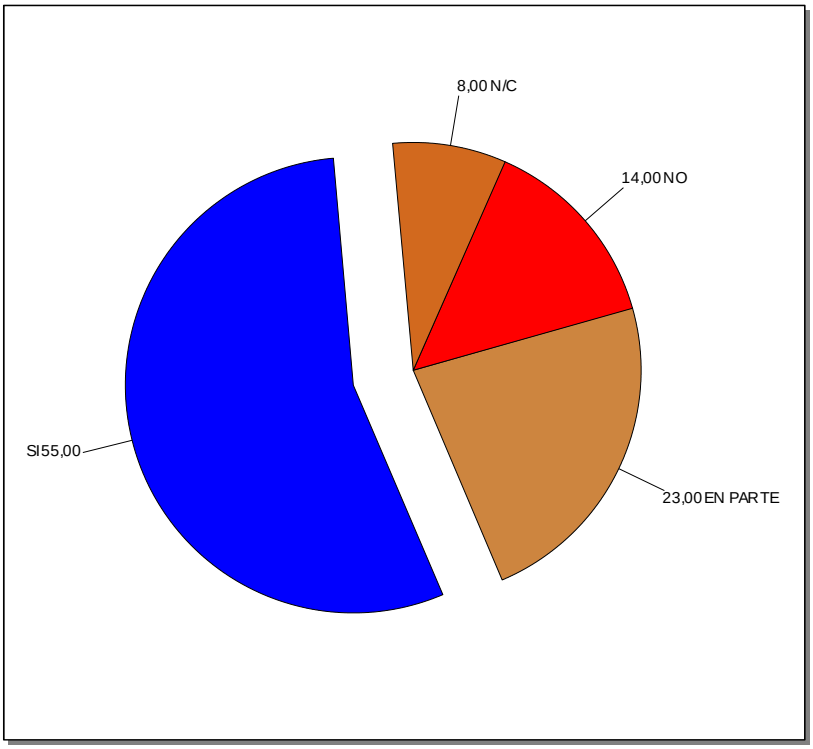


Figura 4.68 Gráfico de Resultado de Servicios inalámbricos (Bluetooth, WIFI, WIMAX)
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. De las personas encuestadas indicaron un 22 % que no posee conocimientos sobre la mala Utilización de Herramientas Tecnológicas con la finalidad de utilizarlas para actividades ilícitas que constituye delito con aplicación de las TICS y que afecta a nuestra actual sociedad en la Administración de Justicia; mientras un 78 % manifestaron que si tienen conocimiento sobre esta temática.

Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

RESULTADOS FORMULARIO 4 (F4): Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

1. **¿Usted tiene conocimiento de computación?**

	P1 Usted tiene conocimiento de computación	(1) SI	57
		(2) EN PARTE	22
		(3) NO	16
		(4) N/C	5
		Total Base sujetos (Conocimiento computación)	100

Tabla 4.69 Cuadro de Resultado de conocimiento de computación
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

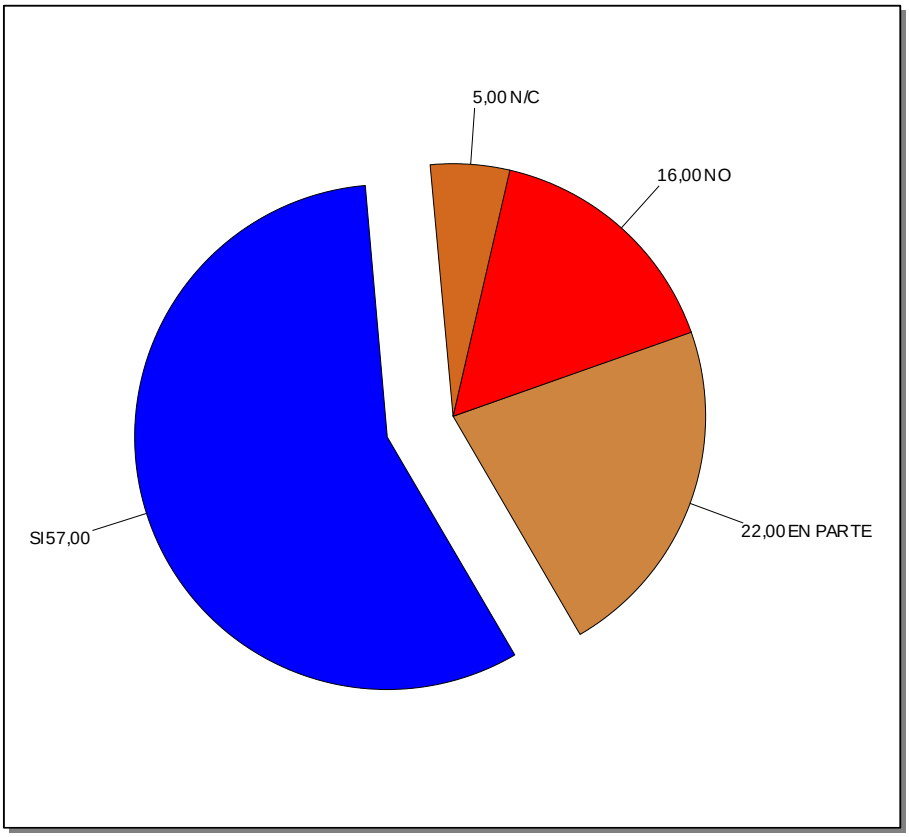


Figura 4.69 Gráfico de Resultado de conocimiento de computación
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 21 % que no tenían conocimientos básicos de computación; mientras un 79 % manifestaron que no es así. La Instituciones deben orientar su planificación y malla curricular desde los niveles más básicos de estudios informáticos para la población en general.

2. ¿Conoce sobre la herramienta de internet?

	P2 Conoce sobre la herramienta de internet	(1) SI	53
		(2) EN PARTE	23
		(3) NO	17
		(4) N/C	7
		Total Base sujetos (Herramienta de internet)	100

Tabla 4.70 Cuadro de Resultado de sobre la herramienta de internet
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

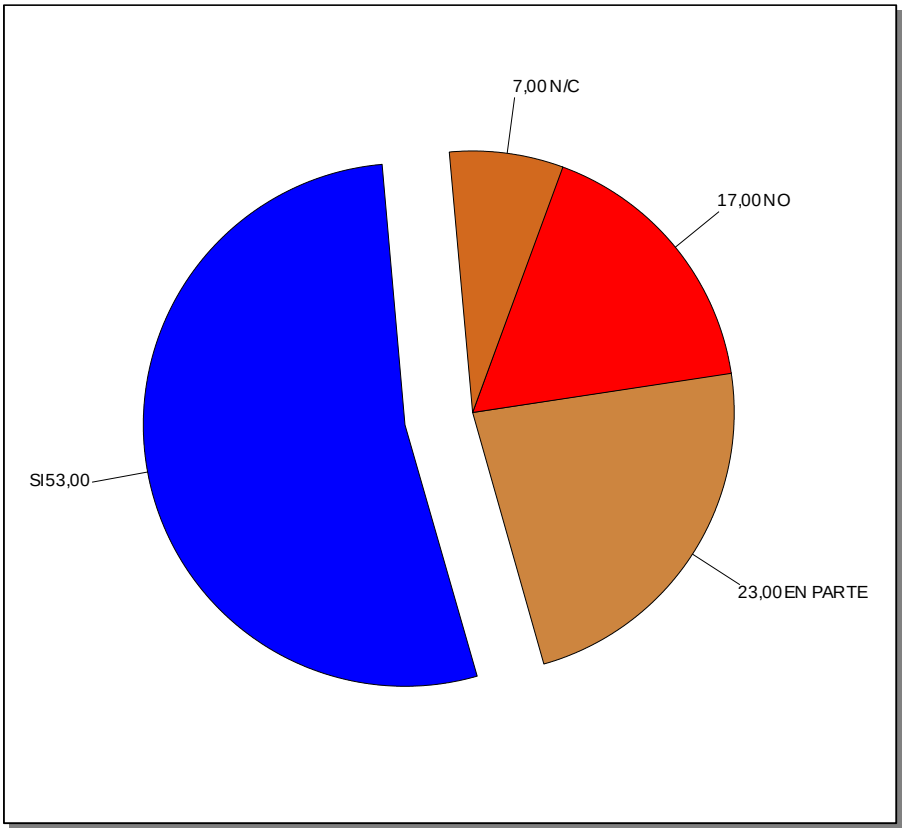


Figura 4.70 Gráfico de Resultado de sobre la herramienta de internet
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 24 % que no tenían experiencia en manejo de entornos de Internet; mientras un 76 % manifestaron que si tenían experiencia.La Instituciones deben orientar su planificación y malla curricular desde los niveles más básicos de estudios informáticos para la población en general.

3. ¿Maneja internet?

	P3 Maneja internet	(1) SI	49
		(2) EN PARTE	28
		(3) NO	15
		(4) N/C	8
		Total Base sujetos (Maneja internet)	100

Tabla 4.71 Cuadro de Resultado del manejo de internet
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

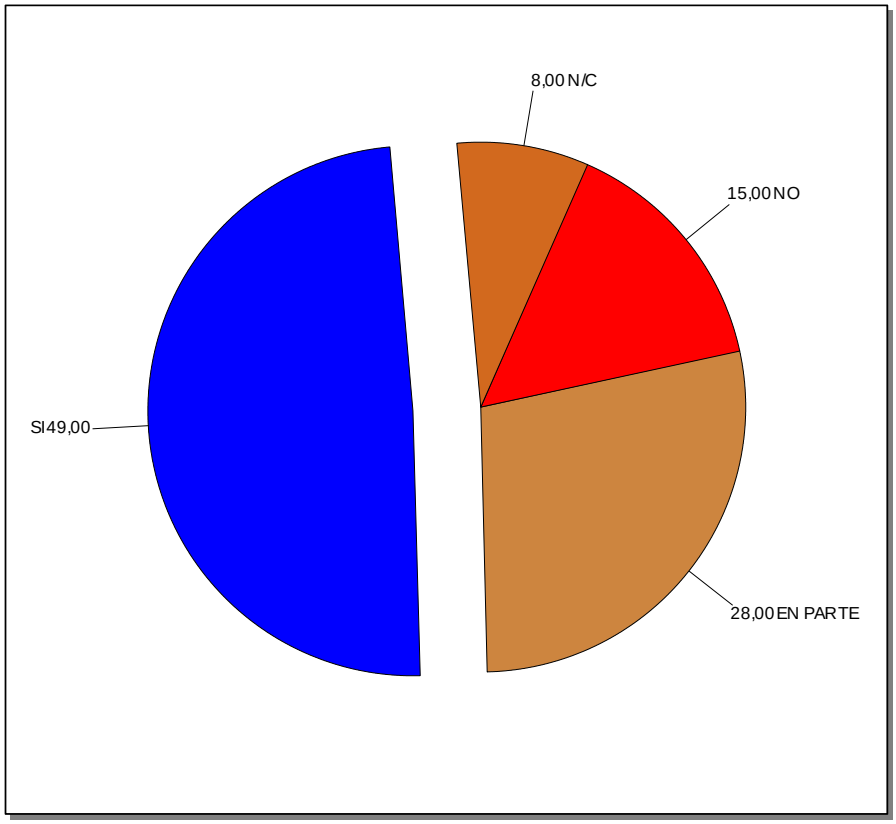


Figura 4.71 Gráfico de Resultado del manejo de internet
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 23 % que no tenían experiencia en manejo de entornos de Internet; mientras un 77 % manifestaron que si tenían experiencia. Las Instituciones deben orientar su planificación y malla curricular desde los niveles más básicos de estudios informáticos para la población en general.

4. ¿Sabe usted que es un delito informático?

	P4 Sabe usted que es un delito informático	(1) SI	19
		(2) EN PARTE	19
		(3) NO	53
		(4) N/C	9
		Total Base sujetos (Informático)	100

Tabla 4.72 Cuadro de Resultado de conocimiento sobre Delito Informático. Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

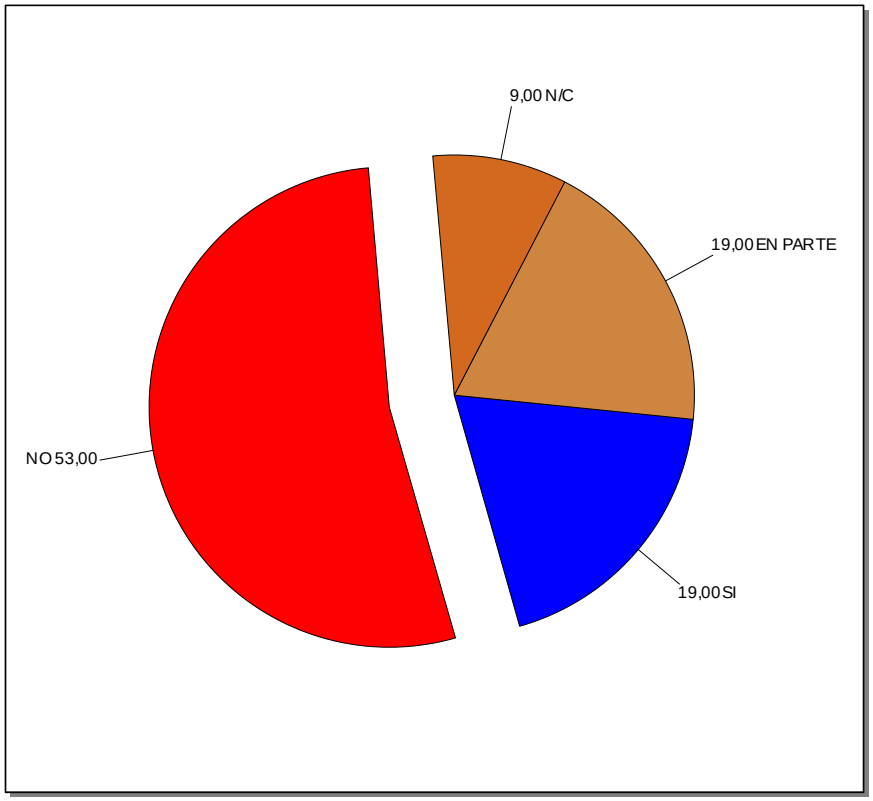


Figura 4.72 Gráfico de Resultado de conocimiento sobre Delito Informático. Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 62 % que no tenían conocimiento de Delitos Informáticos; mientras un 38 % manifestaron que si tenían conocimiento. Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

5. ¿Sabe cuáles son los principales delitos informáticos?

	P5 Sabe cuales son los principales delitos informáticos	(1) SI	17
		(2) EN PARTE	22
		(3) NO	54
		(4) N/C	7
		Total Base sujetos (Informáticos)	100

Tabla 4.73 Cuadro de Resultado de conocimiento de los principales delitos informáticos.
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

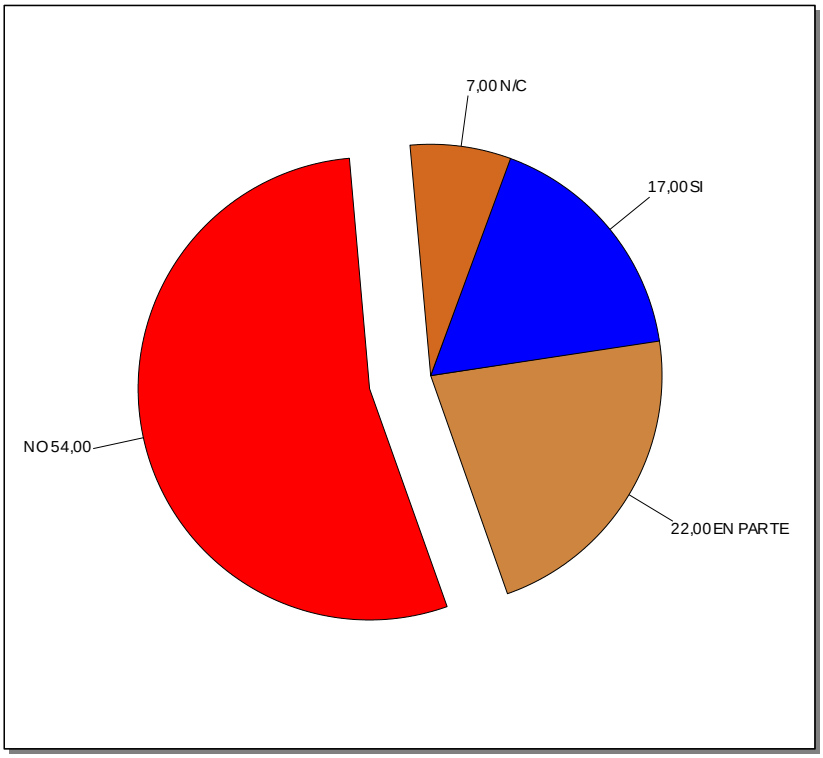


Figura 4.73 Gráfico de Resultado de conocimiento de los principales delitos informáticos.
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 61 % que no tenían conocimiento de los principales Delitos Informáticos que afectan a nuestra actual sociedad; mientras un 39 % manifestaron que si tenían conocimiento. Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que

necesita la sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

6. ¿Ha sido víctima de algún delito informático?

	P6 Ha sido víctima de algún delito informático	(1) SI	23
		(2) EN PARTE	18
		(3) NO	51
		(4) N/C	8
		Total Base sujetos (Informático)	100

Tabla 4.74 Cuadro de Resultado de victimas de delitos informáticos. Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

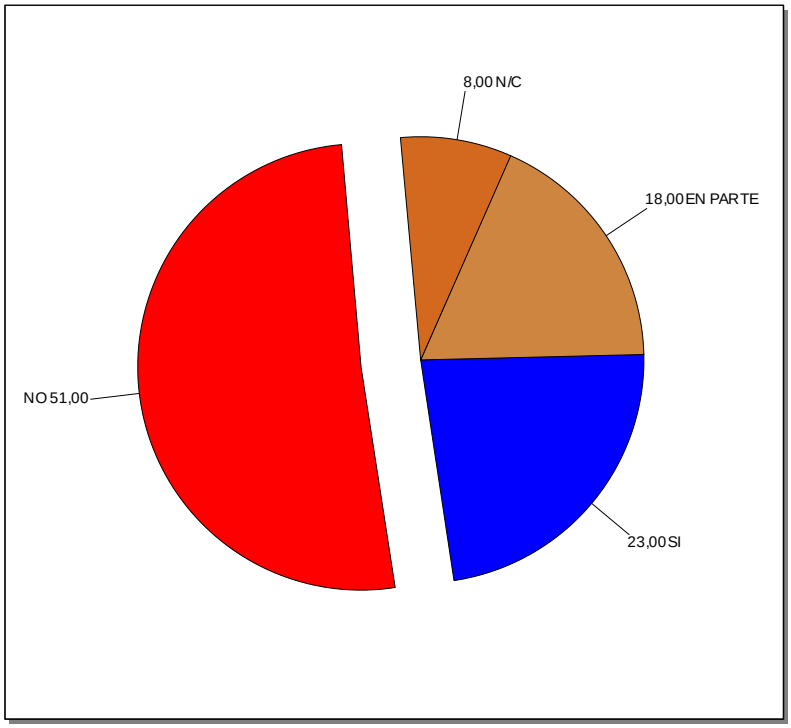


Figura 4.74 Gráfico de Resultado de victimas de delitos informáticos. Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 59 % que no han sido víctimas de algún Delito Informático; mientras un 41 % manifestaron que si han sido afectados.

Las Instituciones que regulan deben orientar a la sociedad en el reconocimiento y formas de atención de los Delitos utilizando las TICS; sobre todo debido a que es un área que está en continuo desarrollo.

7. ¿Sabe dónde dirigirse en el caso de ser víctima de algún delito informático?

	P7 Sabe dónde dirigirse en el caso de ser víctima de algún delito informático	(1) SI	22
		(2) EN PARTE	19
		(3) NO	52
		(4) N/C	7
		Total Base sujetos (Informático)	100

Tabla 4.75 Cuadro de Resultado de conocimiento de donde dirigirse por ser victima de algún delito informático
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

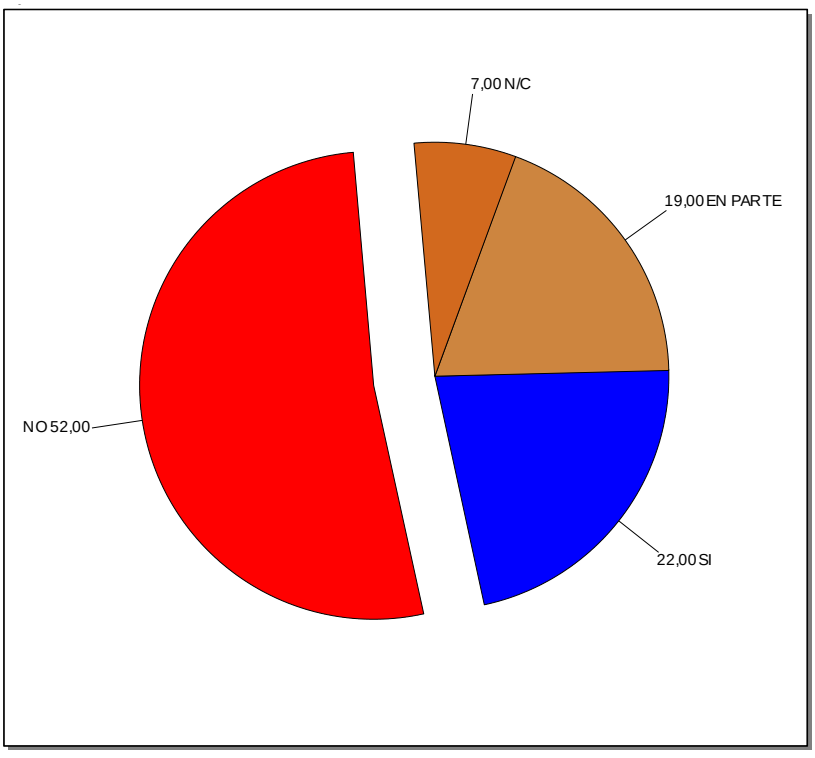


Figura 4.75 Gráfico de Resultado de conocimiento de donde dirigirse por ser victima de algún delito informático
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 59 % que no tienen conocimiento a la entidad donde debe dirigirse en el caso de ser víctima de un Delito Informático; mientras un 41 % manifestaron que si tenían conocimiento.

Las Instituciones que regulan deben orientar a la sociedad en el reconocimiento y formas de atención de los Delitos utilizando las TICS; sobre todo debido a que es un área que está en continuo desarrollo.

8. ¿Conoce usted qué es la seguridad informática?

	P8 Conoce usted qué es la seguridad informática	(1) SI	23
		(2) EN PARTE	21
		(3) NO	48
		(4) N/C	8
		Total Base sujetos (Informática)	100

Tabla 4.76 Cuadro de Resultado de Conocimiento sobre Seguridad Informática
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

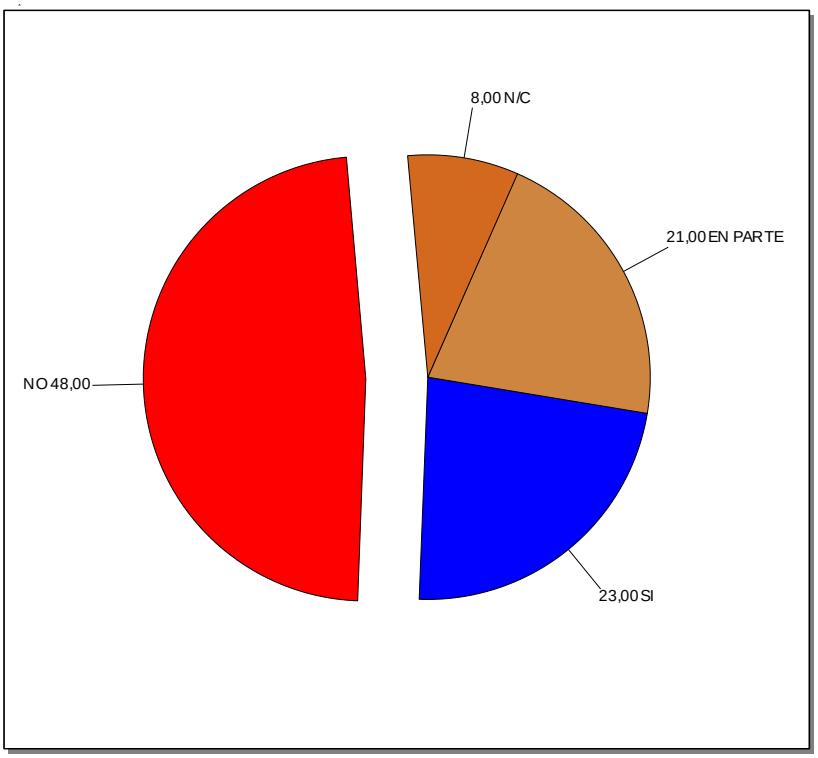


Figura 4.76 Gráfico de Resultado de Conocimiento sobre Seguridad Informática
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 56 % que no conocen lo referente a Seguridad Informática que incide directamente en los Delitos utilizando las TICS que afecta a nuestra actual sociedad; mientras un 44 % manifestaron que si tienen conocimiento. Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de atención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

9. ¿Toma acciones para evitar delitos informáticos?

	P9 Toma acciones para evitar delitos informáticos	(1) SI	22
		(2) EN PARTE	18
		(3) NO	51
		(4) N/C	9
		Total Base sujetos (Informáticos)	100

Tabla 4.77 Cuadro de Resultado de Toma de Acciones para evitar Delito Informático
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

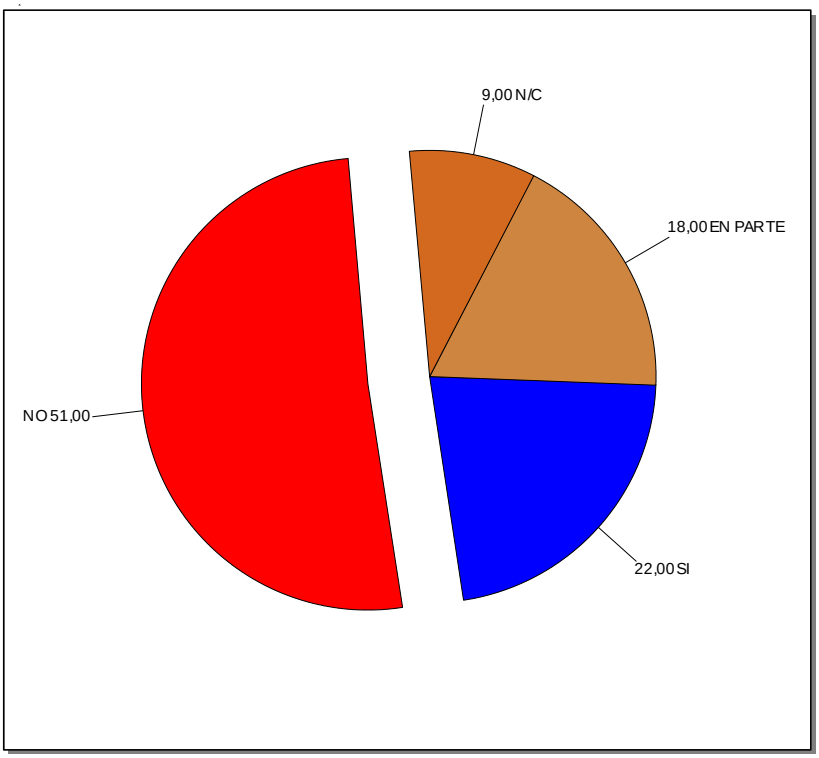


Figura 4.77 Gráfico de Resultado de Toma de Acciones para evitar Delito Informático
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 60 % no toma acciones para evitar Delitos utilizando las TICS que afecta a nuestra actual sociedad; mientras un 40 % manifestaron que si tomaban acciones de prevención.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

10. ¿Ha realizado una transacción electrónica?

	P10 Ha realizado una transacción electrónica	(1) SI	63
		(2) EN PARTE	21
		(3) NO	7
		(4) N/C	9
		Total Base sujetos (Transacción electrónica)	100

Tabla 4.78 Cuadro de Resultado de Uso de Transacciones Electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

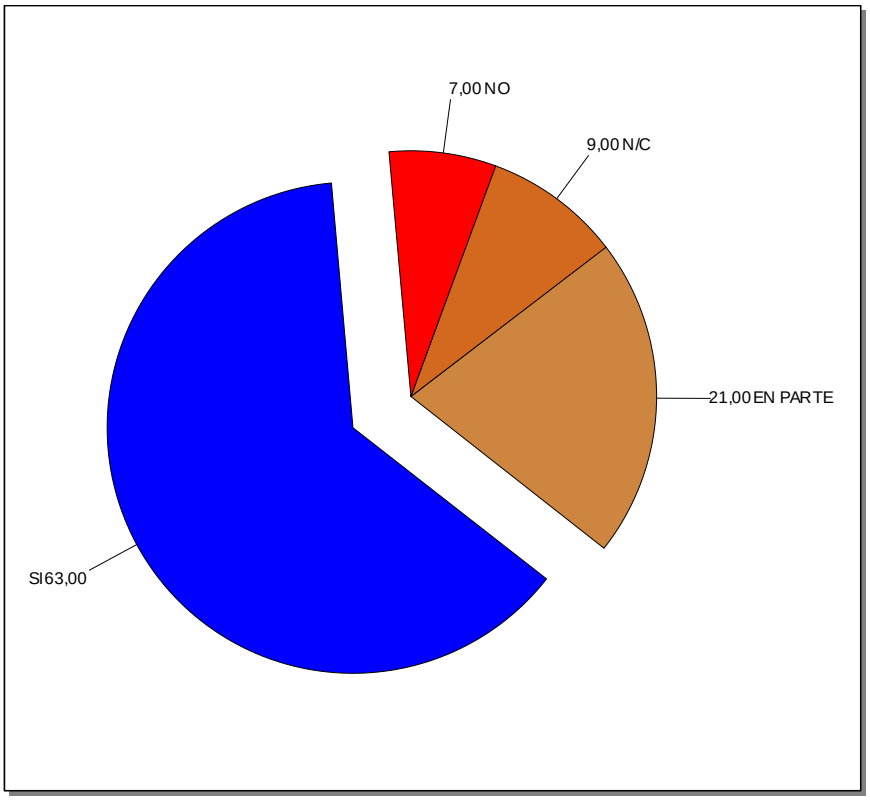


Figura 4.78 Gráfico de Resultado de Uso de Transacciones Electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 16 % que no conoce ni ha realizado transacciones electrónicas en los Portales de Internet como elemento vinculado a las TICS y que constituye un nuevo servicio comercial con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 84 % manifestaron que si toman precauciones al momento de realizar actividades en Comercio Electrónico.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

11. ¿Siente seguridad al realizar transacciones electrónicas?

	P11 Siente seguridad al realizar transacciones electrónicas	(1) SI	20
		(2) EN PARTE	28
		(3) NO	43
		(4) N/C	9
		Total Base sujetos (Transacciones)	100

Tabla 4.79 Cuadro de Resultado de Seguridad al realizar transacciones electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

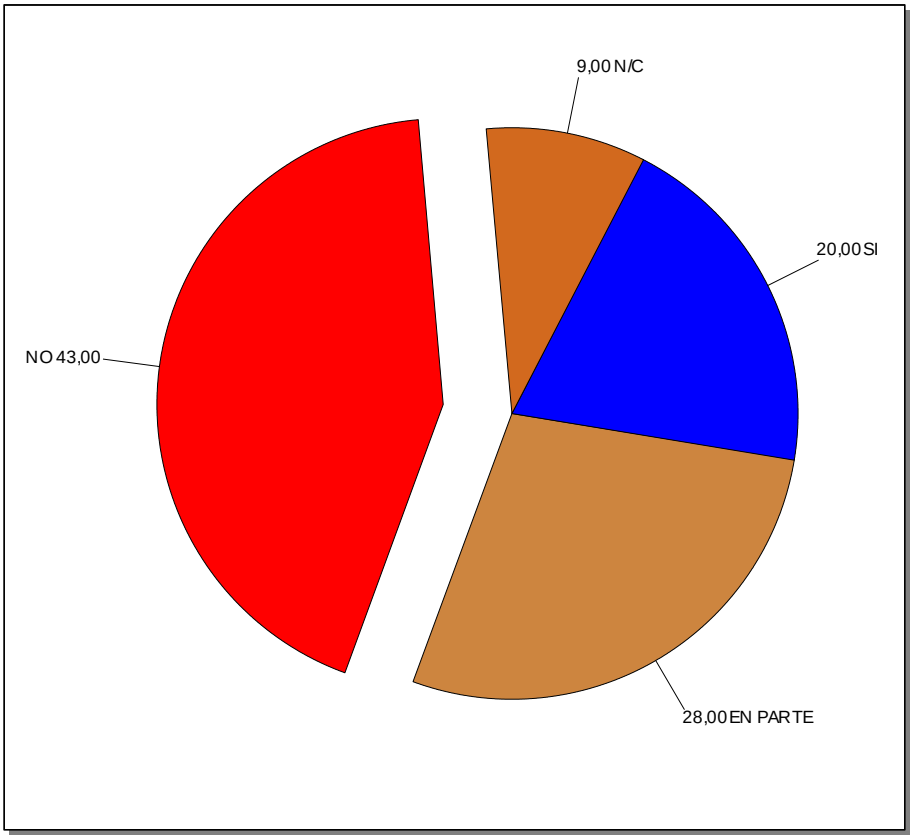


Figura 4.79 Gráfico de Resultado de Seguridad al realizar transacciones electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron en 52 % que no sienten seguridad para realizar transacciones electrónicas en los Portales de Internet como elemento vinculado a las TICS y que constituye un nuevo servicio comercial con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 84 % manifestaron que si tienen confianza al momento de realizar actividades en Comercio Electrónico.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

12. ¿Ha tomado precauciones al realizar transacciones electrónicas?

	P12 Ha tomado precauciones al realizar transacciones electrónicas	(1) SI	52
		(2) EN PARTE	24
		(3) NO	16
		(4) N/C	8
		Total Base sujetos (Precauciones transacciones)	100

Tabla 4.80 Cuadro de Resultado de Precauciones al realizar transacciones electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

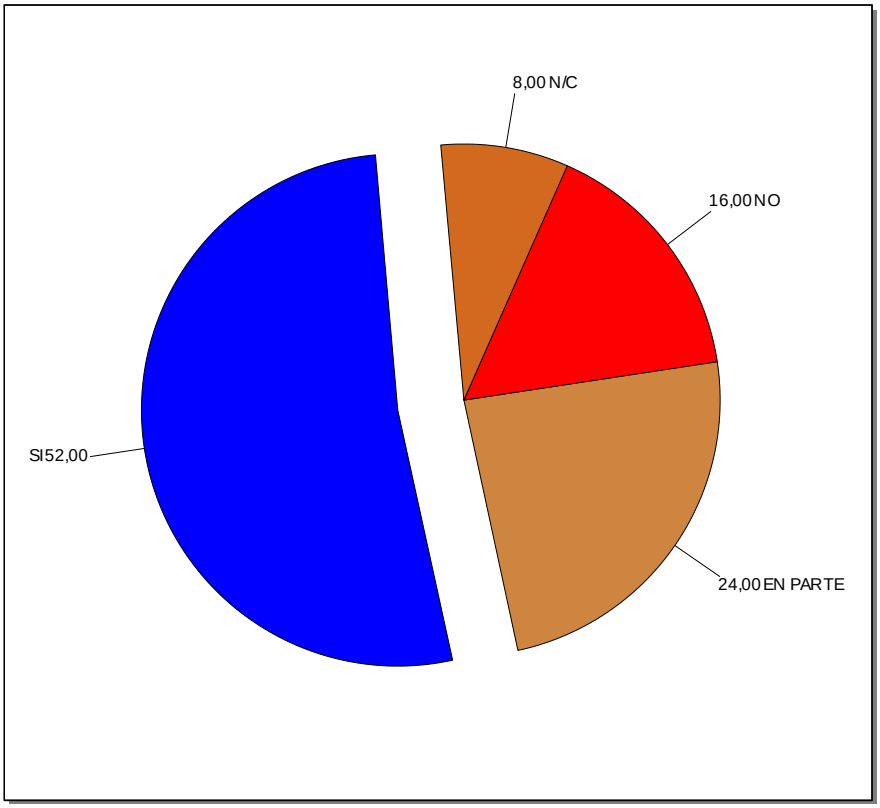


Figura 4.80 Gráfico de Resultado de Precauciones al realizar transacciones electrónicas
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 24 % que no toman precauciones al momento de realizar transacciones electrónicas en los Portales de Internet como elemento vinculado a las TICS y que constituye un nuevo servicio comercial con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras

un 76 % manifestaron que si toman precauciones al momento de realizar actividades en Comercio Electrónico.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

13. ¿Tiene usted correo electrónico?

	P13 Tiene usted correo electrónico	(1) SI	62
		(2) EN PARTE	20
		(3) NO	11
		(4) N/C	7
		Total Base sujetos (Correo electrónico)	100

Tabla 4.81 Cuadro de Resultado de Correo Electrónico
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

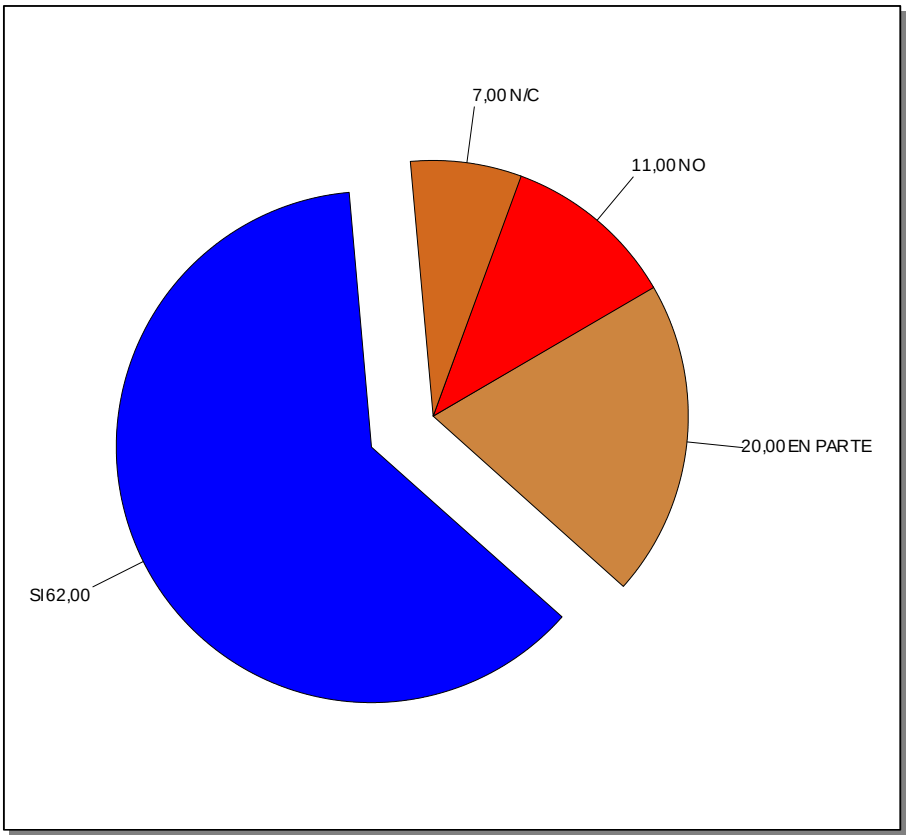


Figura 4.81 Gráfico de Resultado de Correo Electrónico
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 18 % que no posee un correo electrónico ni personal ni corporativo y que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 82 % manifestaron que si lo poseen.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

14. ¿Utiliza con frecuencia su correo electrónico?

	P14 Utiliza con frecuencia su correo electrónico	(1) SI	25
		(2) EN PARTE	20
		(3) NO	44
		(4) N/C	11
		Total Base sujetos (Frecuencia electrónico)	100

Tabla 4.82 Cuadro de Resultado de Frecuencia de utilización de correo electrónico.
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

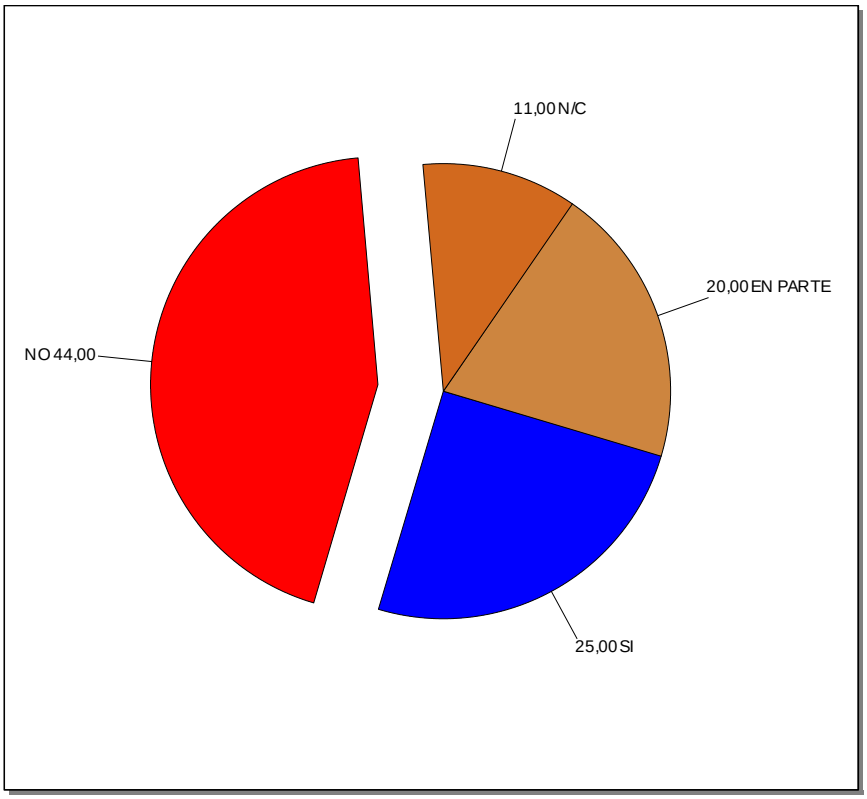


Figura 4.82 Gráfico de Resultado de Frecuencia de utilización de correo electrónico.
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 55 % que no utilizaba el correo electrónico ni personal ni corporativo con frecuencia y que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 45 % manifestaron que si lo utilizan.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

15. ¿Alguna vez ha sido bloqueado su correo electrónico?

	P15 Alguna vez ha sido bloqueado su correo electrónico	(1) SI	22
		(2) EN PARTE	20
		(3) NO	51
		(4) N/C	7
		Total Base sujetos (Electrónico)	100

Tabla 4.83 Cuadro de Resultado de Bloqueo de correo electrónico
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

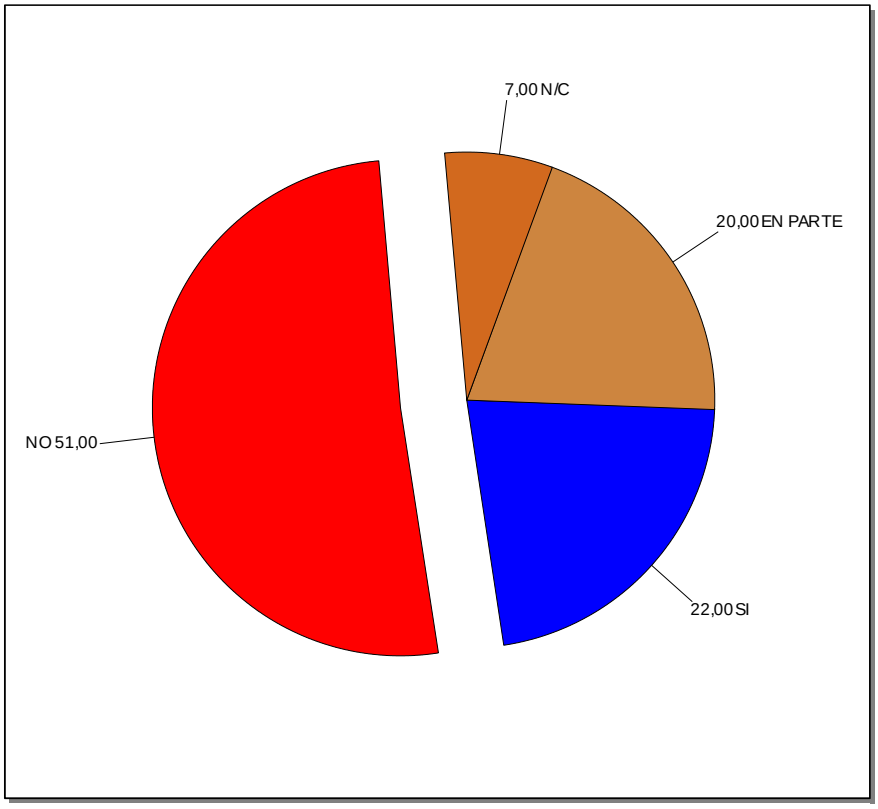


Figura 4.83 Gráfico de Resultado de Bloqueo de correo electrónico
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 58 % que no se le ha bloqueado el correo electrónico ni personal ni corporativo; que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 42 % manifestaron que si se le ha bloqueado su correo. Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

16. ¿Pese a los problemas actuales sobre los delitos informáticos utilizaría o seguiría utilizando servicios vía web?

	P16 Pese a los problemas actuales sobre los delitos informáticos utilizaría o seguiría utilizando servicios vía web	(1) SI	20
		(2) EN PARTE	18
		(3) NO	52
		(4) N/C	10
		Total Base sujetos (Informáticos)	100

Tabla 4.84 Cuadro de Resultado de Utilización de Servicios Web
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

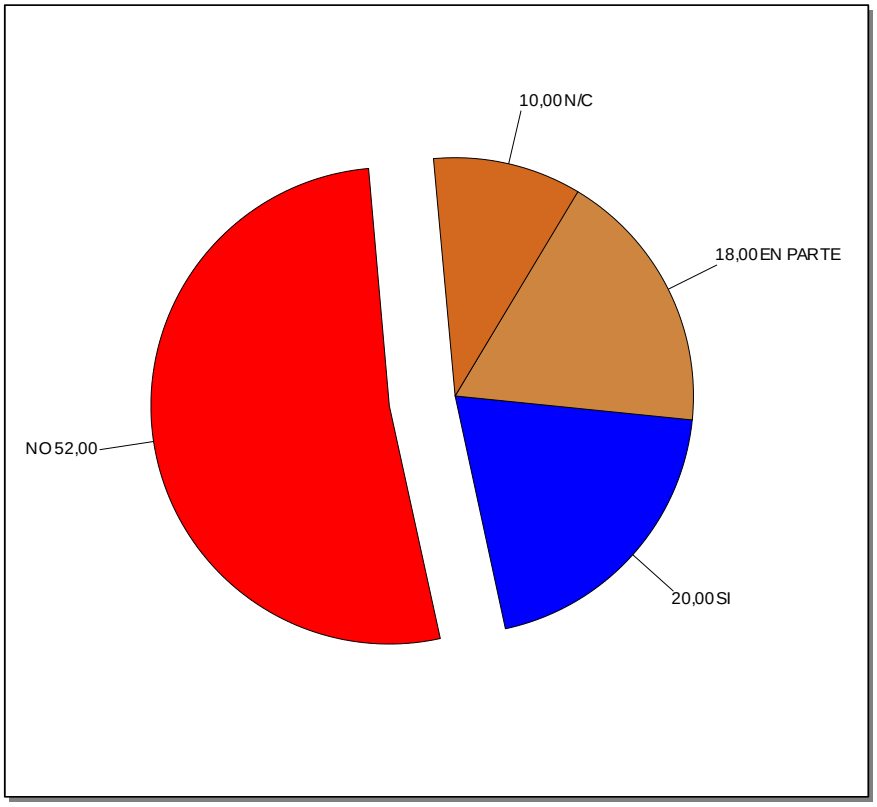


Figura 4.84 Gráfico de Resultado de Utilización de Servicios Web
Fuente: Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. De las personas encuestadas indicaron un 63 % que no utilizarían ningún servicio electrónico por motivos que existen actualmente de los Delitos Informáticos; que constituye un nuevo servicio con aplicación de las TICS y que afecta a nuestra actual sociedad; mientras un 37 % manifestaron que si brindarían confían en la utilización de servicios vía web.

Las Instituciones deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS.

4.1.1.1 Resultado de la Entrevista

Cuestionario

Codigo	Pregunta	Opciones	Respuestas
P1	¿Tiene conocimiento si existen acciones procedimentales a seguir contra los Delitos Informáticos en el Ecuador?		Si
P2	¿Cuáles son las acciones procedimentales a seguir contra los Delitos Informáticos en el Ecuador?		Sanciones; incurrirá en prisión de uno (1) a seis (3) mes multa de cinco (5) a veinte (6) salarios mínimos legales mensuales vigentes.
P3	¿Tiene conocimiento si existen procedimientos a seguir para la recolección de evidencias contra los Delitos Informáticos en el Ecuador?		Si
P4	¿Cuáles son los procedimientos a seguir para la recolección de evidencias contra los Delitos Informáticos en el Ecuador?		Cadena de Custodia.
P5	¿En la actualidad existen mecanismos de juzgamiento para resolver los delitos informáticos?		Si;
P6	¿Cuáles son los mecanismos de juzgamiento para resolver los delitos informáticos?		En el ambito penal; el hurto, robo, fraude
P7	¿Sabe usted dónde se dirigen las personas afectadas por delitos informáticos?		Fiscalia
P8	¿Cree usted que los jueces cuentan con un buen nivel de conocimiento sobre las TICS?		No
P9	¿Cree usted que los jueces cuentan con una visión clara sobre los delitos informáticos?		No
P10	¿Cree usted que los autores de delitos informáticos en el país cuentan con un alto nivel de conocimiento sobre las TICS?		Si
P11	¿Cree usted que las entidades que ofrecen servicios informáticos cuentan con un buen nivel de seguridad informática?		No
P12	¿En la actualidad se cuenta con procedimientos para regular los delitos informáticos?		No
P13	¿Cuáles son los procedimientos para regular los delitos informáticos?		Ninguno
P14	¿En la actualidad se cuenta con planes de acción para regular los delitos informáticos?		NO
P15	¿Cuáles son los planes de acción para regular los delitos informáticos?		Ninguno
P16	¿Cuáles son los principales delitos informáticos que actualmente se están realizando?		Robo de Entidad, Phishing, Amenazas de muerte, Pedofilia, Vulnerizaciones de los sitios web de las
P17	¿Sabe usted cuál es el grupo social más afectado por causa de los delitos informáticos?		Media y Alta
P18	¿Para su criterio actualmente se están resolviendo con éxito los delitos informáticos?		No
P19	¿Por su conocimiento cuál es el mayor impedimento para resolver rápidamente y con éxito los delitos informáticos?		Falta de conocimiento en el procedimiento para llevarlo cabo.
P20	¿Cómo usted piensa que se podría reducir los casos de delitos informáticos?		Mayor educacion a los usuarios final, creando concien en las empresas la seguridad informàtica.

Tabla 4.85 Cuadro de Preguntas a los Especialistas que Resuelven Delitos Informáticos
Fuente: Datos tomados de la entrevista con el Ing. Roberto Olaya – Experto en Delitos Informáticos.

0:06:52

Cuestionario

Codigo	Pregunta	Opciones	Respuestas
P1	¿Cuál es el motivo principal que le motiva a cometer delitos informáticos?		El ego
P2	¿Cuáles son los principales delitos informáticos que usted ha realizado o realiza?		Pago de pensión de la UniversidadEntrar al correo de la noviaAlteraciones de notas
P3	¿De qué vulnerabilidades en los sitios web se vale para cometer los delitos informáticos?		sql injection, cross site script xss, programas de paginas web
P4	¿Qué tiempo lleva cometiendo delitos informáticos?		4 años
P5	¿Cual fue el primer delito informático que cometió?		Cambiar notas en la universidad
P6	¿Con que frecuencia comete delitos informáticos?		2 veces al año
P7	¿Cuándo y cuál fue el último delito informático que cometió?		5 a 6 años aproximadamente, entrar a un correo ajeno
P8	¿Utiliza algún software para cometer los delitos informáticos?		No
P9	¿Utiliza algún hardware para cometer los delitos informáticos?		No
P10	¿Usted trabaja solo o acompañado para cometer los delitos informáticos?		Solo
P11	¿Usted realizo o realiza algún estudio determinado para cometer los delitos informáticos?		Si estudio la infraestructura
P12	¿Cuándo cometió un delito informático en algún momento hubo una oportunidad a que lo descubrieran?		Si hubo.
P13	¿En el momento de cometer un delito informático, cuales son las medidas principales que realiza para no ser descubierto?		Conocer a la persona, o el ambiente, hacerlo en ambien linux y en lugares apartados y que no sea concurrente.
P14	¿Piensa en algún momento dejar de cometer delitos informáticos?		Si
P15	¿Cuál sería el motivo principal por el cual usted dejaría de cometer delitos informáticos?		Madurez, miedo.

Tabla 4.86 Cuadro de Preguntas a los Especialistas que Cometen Delitos Informáticos
Fuente: Datos tomados de la entrevista con el Ing. Roberto Olaya – Experto en Delitos Informáticos.

4.1.2 Discusión de Resultados

4.1.2.1 Verificación de Hipótesis

Los conceptos anteriormente analizados en consecuencia permiten la comprobación de las hipótesis planteadas.

4.1.2.1.1 Contestación de Hipótesis Planteadas

Resultados globales del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

	F1 Cuestionario básico de conocimientos de tics del personal de instituciones de administración de justicia.	SI	37
		EN PARTE	20
		NO	34
		N/C	9
		Total Base sujetos (Conocimientos administración)	100

Tabla 4.87 Cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

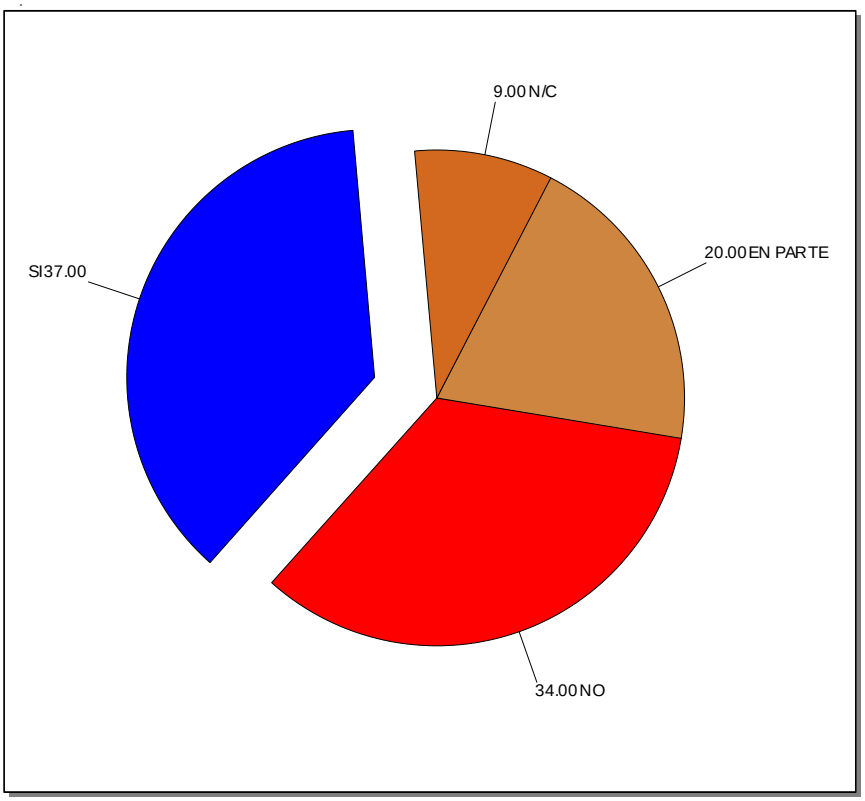


Figura 4.85 Gráfico de Resultado de Utilización de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia
Fuente: Datos tomados del cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. Según los resultados de las encuestas nos damos cuenta que el 37% del personal de Instituciones de Administración de Justicia si tiene conocimiento de Tics y el 34% no lo tiene.

Por lo que es importante que las Instituciones tecnológicas superiores deban orientar su planificación y malla curricular desde los niveles más básicos, conocimiento de Tics para la población de áreas jurídicas. Ya que el porcentaje de no conocimiento es elevado, constituyendo una falencia para el desarrollo de sus funciones.

Resultados globales del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

	F2 Cuestionario de conocimientos jurídicos sobre el marco legal del personal de instituciones de administración de justicia	SI	32
		EN PARTE	19
		NO	40
		N/C	9
		Total Base sujetos (Conocimientos administración)	100

Tabla 4.88 cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia
Fuente: Datos tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

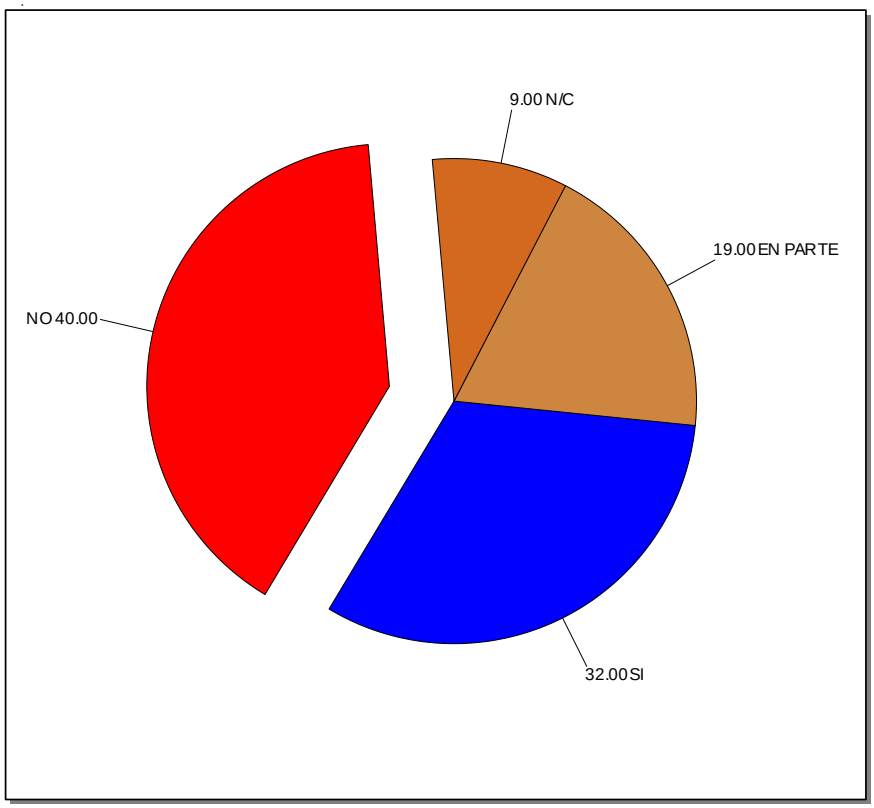


Figura 4.86 Gráfico de Resultado de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia Fuente: Datos tomados del cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

ANÁLISIS. Según los resultados de las encuestas nos damos cuenta que el 32% del personal de Instituciones de Administración de Justicia si tiene conocimientos jurídicos sobre el marco legal y el 40% no lo tiene.

Por lo que es importante que las Instituciones tecnológicas superiores deban orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos utilizando las TICS que vulneran la Seguridad o el buen uso de herramientas tecnológicas en las Instituciones en nuestra sociedad; sobre todo debido a que es un área que está en continuo desarrollo.

Resultados globales del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

	F3 Cuestionario de conocimientos técnicos sobre informática	SI	49
		EN PARTE	23
		NO	21
		N/C	7
		Total Base sujetos (Cuestionario conocimientos)	100

Tabla 4.89 Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

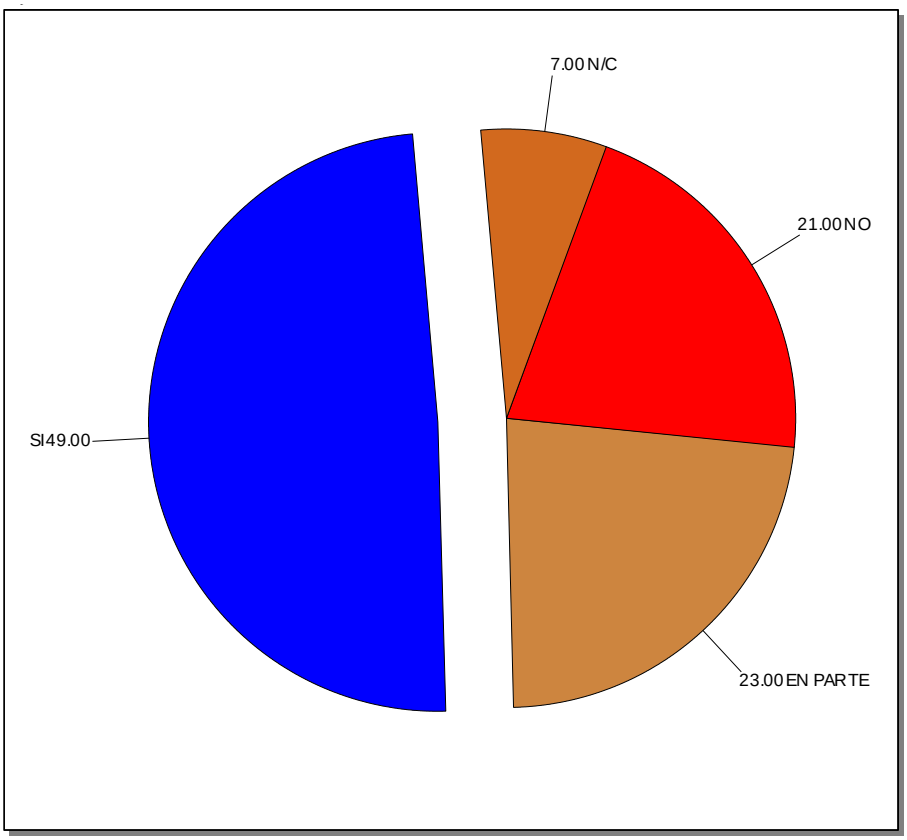


Figura 4.87 Gráfico de Resultado de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico.

ANÁLISIS. Según los resultados de las encuestas nos damos cuenta que el 42% del personal de Instituciones de Administración de Justicia si tiene conocimientos técnicos sobre informática y el 21% no lo tiene.

Sería muy bueno que se refuerce los conocimientos técnicos sobre informática, para mejorar su nivel profesional y ver mayores resultados en el desarrollo de sus actividades.

Resultados globales del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos

	F4 Comercio electrónico y delitos informáticos	SI	34
		EN PARTE	21
		NO	37
		N/C	8
		Total Base sujetos (Electrónico informáticos)	100

Tabla 4.90 Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

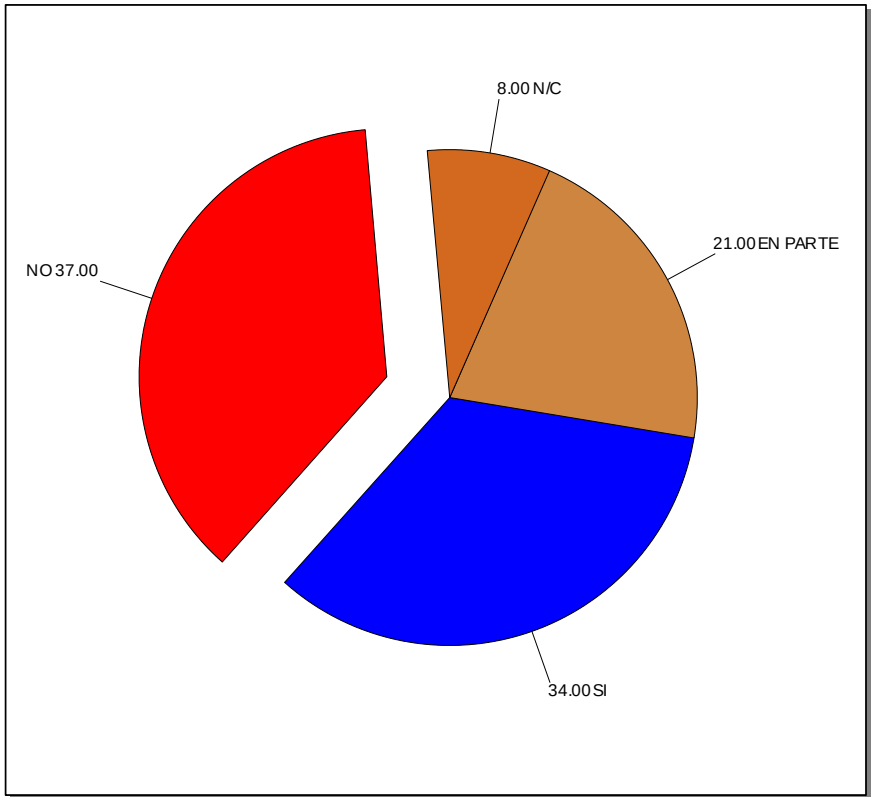


Figura 4.88 Gráfico de Resultado de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos
Fuente: Datos tomados del cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones, Comercio Electrónico y Delitos Informáticos.

ANÁLISIS. Según los resultados de las encuestas nos damos cuenta que el 34% de la sociedad si tiene conocimiento sobre comercio electrónico y delitos informáticos y el 37% no lo tiene.

Nos damos cuenta que el nivel de no conocimiento es mayor, por lo que es importante fomentar el conocimiento de estos temas a la sociedad, ya que se encuentran desprotegidos ante los delitos informáticos.

En conclusión se ha develado en las encuestas y entrevistas la inexistencia de acciones procedimentales y planes bien establecidos para resolver los casos de delitos informáticos. La falta de conocimiento sobre herramientas para adquirir, preservar y recuperar evidencias digitales, además que los jueces no tienen adiestramiento para manejar estas evidencias.

Se puede evidenciar la desconfianza de las personas al realizar transacciones digitales. Por lo que cada vez más personas se van resistiendo al uso de los servicios informáticos.

El vacío de conocimiento y procedimientos que se ha reflejado en las encuestas y entrevistas, cuyos resultados demuestran que falta mucho por hacer para preparar a los integrantes de la Administración de Justicia de Guayaquil, confirma la importancia de la propuesta del Diseño de nuevo esquema para el procedimiento de indagación de los delitos informáticos:

- Estableciendo los requerimientos mínimos necesarios para que la entidad pueda ejercer sus actividades de una manera eficiente, contando con funciones bien definidas según las necesidades actuales y con los recursos con los que se cuentan.

- Estableciendo procesos y procedimientos que permitan controlar las funciones, realizar monitoreo, permitiendo que la entidad trabaje de una manera eficiente, explotando todos los recursos con los que se cuenta.

.

CAPITULO 5

DISEÑO DE NUEVO ESQUEMA PARA EL PROCEDIMIENTO DE INDAGACIÓN DE LOS DELITOS INFORMÁTICOS.

5.1 Introducción

La necesidad de la Administración de Justicia requiere de procedimientos bien establecidos, que le permitan un conocimiento más profundo de los casos que se necesitan analizar, ya que se necesita garantizar la eficacia en el proceso de indagación.

Por lo expuesto, es clave que el personal responsable del proceso de indagación de los delitos informáticos, acredite experiencia, conocimientos teóricos y prácticos, habilidades en la aplicación de los procedimientos.

Esta propuesta sirve para mejorar el procedimiento de indagación de los delitos informáticos. En conjunto con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los criterios y medidas contempladas.

Haciendo imprescindible conocer cada uno de los proceso y funciones de cada uno de los participantes en la indagación de los delitos**,** y que estos puedan resolver de una manera ágil y precisa los casos de delitos informáticos. Que cuenten con la preparación y pericia requerida para identificar, recoger, analizar, y reportar evidencia digital como participantes en la Administración de Justicia en la Sociedad Ecuatoriana.

Se da a conocer cuáles son los elementos, componentes, las diligencias y/o documentos, habilitantes en el proceso de indagación. El diseño pretende mejorar el manejo en la administración de justicia ante los delitos informáticos en nuestro medio.

Se identifica cuáles son los retos (legales, tecnológicos, etc.) que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de indagación.

El esquema de indagación de delitos informáticos, exige una precisa determinación de las causas y el contexto en el cual se plantea. Estos a su vez están condicionados por el cambio fundamental que ha acontecido en las relaciones entre la Administración de Justicia y la Sociedad en función de los Cambios Tecnológicos.

5.2 Esquema del Proyecto

En el esquema para el procedimiento de indagación de los delitos informáticos se incluye las siguientes especificaciones:

- Funciones y Requerimientos mínimos necesarios para indagar y resolver los delitos informáticos.

- Procesos y procedimientos necesarios para indagar y resolver los delitos informáticos.

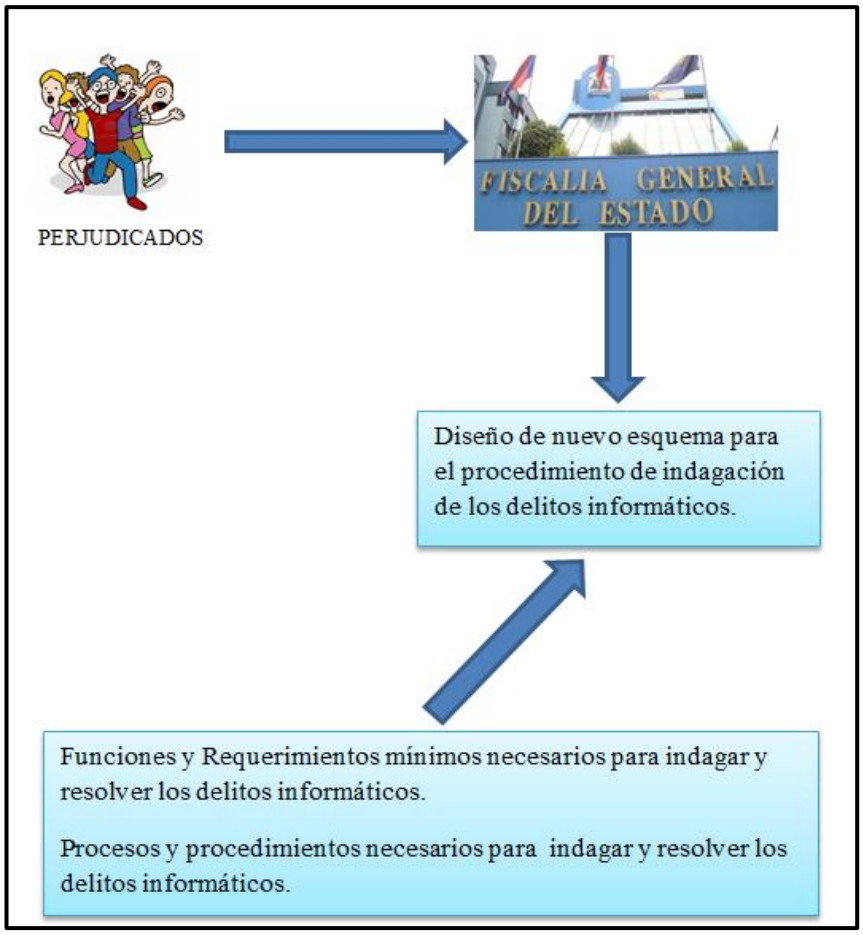


Figura 5.1 Esquema del Proyecto

Fuente: Autores

5.3 Desafíos de la Propuesta

Uno de los mayores desafíos de los delitos electrónicos para el cumplimiento de la ley es la ausencia de fronteras geográficas. Aunque Internet ha eliminado las fronteras de investigación. Las autoridades y los delincuentes, aún están ligados estrechamente por las áreas jurisdiccionales. Estas restricciones de límites y el conflicto resultante de la autoridad a menudo significan que los funcionarios deben solicitar órdenes en múltiples jurisdicciones. Este proceso se puede traducir en una pérdida de tiempo valioso y, en definitiva, pérdida de la evidencia.

Otro impedimento para la persecución del delito cibernético de los casos es el tiempo necesario para que los proveedores de servicios Internet (ISP) respondan a las citaciones. En la actualidad, a menudo toma varias semanas para que un ISP pueda producir los registros citados.

Muchos jefes de policía, los altos directivos, y los que hacen la financiación y la asignación de recursos no poseen el nivel de conocimientos o herramientas necesarias para investigar y preparar los casos para su enjuiciamiento exitoso.

5.3.1 Los Obstáculos a la Identificación de los Hacker

Debido a la composición de la Internet, a veces es difícil para los investigadores descubrir la identidad de un hacker.

- Un hacker podría ocultar o "falso" el Protocolo de Internet (IP), o de forma intencionada podría subir sus comunicaciones a través de muchos ordenadores intermedios dispersos por el mundo antes de llegar a un equipo de destino. Luego el investigador debe identificar todos los puntos intermedios para encontrar la ubicación de los hackers. Citaciones y órdenes judiciales de cada punto de rebote puede ser necesario para identificar al hacker.

- Debido al anonimato que ofrece Internet, un hacker puede reclamar sospecha de que alguien utilizó su equipo y asumió su identidad en el momento del ataque.

- Algunas de las víctimas no llevan un registro o no descubren las actividades de un hacker hasta que es demasiado tarde para obtener registros de proveedor de los hackers de servicios de Internet (ISP).

- Algunos ISP no llevan registros para ser de ayuda a los investigadores. Cuando el investigador determina la identidad de un ISP y que registros serán necesarios, el fiscal deberá enviar una carta que requiere el ISP para preservar los registros mientras que el proceso de una orden judicial.

- Algunos hackers alteran los registros a obtener acceso no autorizado, el cual oculta la evidencia de sus crímenes.

- Algunas pistas pasan por otros países, no todos consideran que la piratería es un delito. Los tratados, convenios y acuerdos están en vigor con algunos países, contactos en decenas de países alrededor del mundo que puede ser contactado en busca de ayuda.

5.4 Manual de Procesos, Funciones y Requerimientos Mínimos para Indagar y Resolver los Delitos Informáticos

El manual cuenta con procesos, procedimientos y funciones bien definidas según las necesidades actuales, se establece los requerimientos mínimos necesarios para que la entidad encargada de resolver los delitos pueda ejercer sus actividades de una manera eficiente.

5.4.1 ¿Cómo se debe Investigar?

Solo se puede reunir información de propiedad sobre un incidente de la siguiente manera:

- Solicitud de revelación voluntaria de información.
- Mandato judicial.
- Orden de registro.

5.4.2 Procesos para Realizar Investigación de Delitos Informáticos

Para realizar una investigación de delitos informáticos, vamos a dividir en dos procesos: **la búsqueda - captura, y la recuperación de la información**.

Búsqueda / Captura: Se incautara los ordenadores y equipos por la policía, buscando archivos incriminatorios y evidencias de actividad ilegal.

Recuperación de Información: El investigador accederá a fuentes de datos a partir de material recuperado, se puede tratar de una base de datos, archivos de registro o página web.

Inicialmente, los investigadores deben tratar un delito informático como un crimen habitual en que cualquier ubicación física en cuestión es aislada y sólo agentes autorizados pueden entrar en él a medida que examinan el lugar de pruebas y aseguren de que nada es alterado o eliminado.

Los investigadores deben rastrear información incriminatoria a la computadora que dio como resultado la búsqueda y el seguimiento de la dirección IP. La dirección IP es como un número de serie asignado a una computadora que tenga acceso al Internet.

Muchos delincuentes informáticos tienen tácticas particulares o delitos que son conocidos. Así que los investigadores deben revisar las circunstancias del delito actual de los criminales y los hackers que conocen que funcionan de manera similar. Una vez realizada la lista de sospechosos, se investigara cada uno de ellos para determinar quién tenía acceso a la víctima y la capacidad y oportunidad para cometer el delito en cuestión.

Los profesionales capacitados deben interrogar a las víctimas y posibles para comprender el alcance de la delincuencia. Se debe tratar de igualar a un sospechoso con el acto cometido. Con esto se ayuda atar el crimen a otros similares y ver si surge un patrón.

Una vez que existe suficiente evidencia disponible para órdenes y las detenciones, los agentes de campo persiguen al sospechoso sobre las áreas de búsqueda que la legislación lo permita y se realizara los arrestos necesarios.

Dividimos en etapas o procedimientos los procesos de Búsqueda/Captura y Descubrimiento de la Información para un mejor entendimiento en su gestión.

Desarrollar un plan estratégico	Brindar seguridad en la escena del crimen	Observación de la Escena del Crimen	Búsqueda de la evidencia	Recuperar la evidencia	Proceso de pruebas

Tabla #5.1 Procedimientos del Proceso de Búsqueda y Captura

Fuente: Los Autores

Formular el Plan Estratégico	Búsqueda de la evidencia	Proceso de pruebas

Tabla #5.2 Procedimientos del Proceso de Descubrimiento de la Información

Fuente: Los Autores

Encontrar, documentar y recuperar evidencia física puede ser una tarea especialmente difícil, ya que se debe tener cuidado en el manejo de la escena del crimen y el manejo de la evidencia encontrada allí.

Si bien es cierto hay procedimientos en común, pero en el proceso de búsqueda-captura es mucho más complicado. Esto se debe a la búsqueda de la evidencia física, como en computadoras, componentes y medios de comunicación, a diferencia de la evidencia lógica del proceso de descubrimiento de la información. Encontrar, documentar y recuperar evidencia física puede ser una tarea especialmente difícil, ya que se debe tener cuidado en el manejo de la escena del crimen informático y el manejo de la evidencia encontrada.

El proceso de descubrimiento de información no presenta tantos temas, porque es en formato electrónico. Uno podría estar tentado a suponer que el descubrimiento de información se deduce necesariamente de las etapas de búsqueda y captura: por ejemplo, después de localizar una computadora en la escena del crimen, un investigador lleva a cabo actividades sobre el descubrimiento de ese equipo en busca de evidencia lógica en el disco duro. Aunque en concepto suena bien, esto es incorrecto en la práctica.

El proceso de búsqueda y captura, la evidencia del proceso, es donde un

investigador realmente examinar los datos en el disco duro de una computadora de la escena del crimen. La característica distintiva es que el descubrimiento de información no se realiza en los ordenadores incautados, los componentes, o los medios de comunicación. Más bien, es la recuperación de evidencia lógica.

5.4.2.1 Procedimientos del Proceso de Búsqueda y Captura

Formular el Plan Estratégico: El investigador, debe determinar qué pruebas se está buscando, y decide cómo se procederá en la búsqueda de pruebas.

Brindar Seguridad en la Escena del Crimen: Los investigadores llegan a la escena del crimen y deben brindar toda la seguridad para que nada sea alterado por personas no autorizadas.

Observación de la Escena del Crimen: El investigador debe observar cuidadosamente donde los artículos y las pruebas pertinentes se encuentran dentro de la escena del crimen informático.

Búsqueda de Pruebas y Recuperación de evidencia: Respectivamente, los investigadores deben encontrar, empacar y mover datos al laboratorio de preservación de pruebas.

En la búsqueda de pruebas, el investigador accede a repositorios de datos (por ejemplo, archivos de registro, bases de datos, Internet, etc) en un esfuerzo por facilitar la información pertinente al caso.

Proceso de Pruebas: Los investigadores deben gestionar y analizarlas pruebas en un laboratorio de preservación de pruebas.

5.4.2.2 Procedimiento del Proceso de Descubrimiento de Información

Formular el Plan Estratégico: El investigador, debe determinar qué pruebas se está buscando, y decide cómo se procederá en la búsqueda de pruebas.

Búsqueda de pruebas: Consiste en un investigador acceder a repositorios de datos

(por ejemplo, archivos de registro, bases de datos, Internet, etc) en un esfuerzo por facilitar la información pertinente al caso

Proceso de Pruebas: Los investigadores deben gestionar y analizar las pruebas en un laboratorio de preservación de pruebas.

La manera más sólida y rápida de las pruebas de seguimiento y manejo de datos de los casos, es utilizando un sistema de software diseñado para ese propósito. Sin embargo, en ausencia de dinero para comprar, o los medios para construir un sistema, el investigador puede recurrir a otras opciones, menos potente. Por ejemplo, un procesador de hojas de cálculo o de palabra se puede utilizar para crear plantillas de casos que puede ser llenado con la información apropiada durante una investigación.

El software de cifrado, como PGP, proporciona un medio sencillo para obtener la talla de hoja de cálculo, procesador de textos y documentos.

Tomar notas sobre papel, es también una posibilidad, pero no sin inconvenientes pocos desafortunados. En primer lugar, las notas escritas a mano no se pueden conseguir tan fácilmente como archivos electrónicos. Notas escrita a mano no se puede integrar en otras fuentes de información tan convenientemente como archivos electrónicos. Y las notas escritas a mano no pueden ser fácilmente almacenadas en bases de datos para la búsqueda y análisis. Esto no quiere decir que los investigadores deberían evitar escribir cosas en el papel. En cambio, los datos del caso deben ser recogidos en un formato electrónico seguro tan pronto como sea posible. Idealmente, un investigador será capaz de escribir sus notas directamente en un sistema de gestión de casos a fin de que estos datos estén protegidos y puestos a disposición en una base de datos de información sobre el caso. No tan ideal, un investigador puede grabar notas en una hoja de cálculo, procesador de texto, o en papel, pero en algún momento se debe almacenarlas notas en una base de datos de algún tipo.

Cuando los investigadores realizan sus investigaciones de una manera no científica. La evidencia recopilada no se toma demasiado en serio en los tribunales de justicia.

5.4.3 Esquema de los Procesos en una Investigación de Delitos Informáticos

El macroproceso **Investigar Delitos Informáticos** esta desglosado en tres niveles detallados a continuación.

Nivel 1: **Macroproceso**: Investigar Delitos Informáticos.

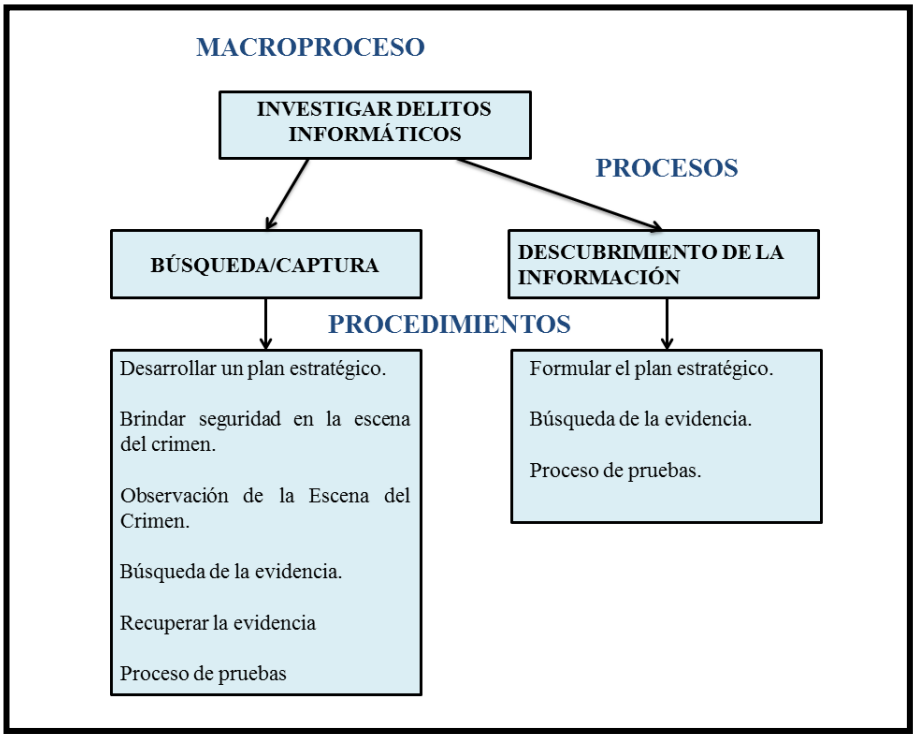


Figura #5.2 Jerarquía del macroproceso investigar delitos informáticos

Fuente: Los Autores

5.4.4 Definición del Proceso Búsqueda – Captura y del Proceso Descubrimiento de Información

Nivel 2: **Procesos**: Búsqueda – Captura y Descubrimiento de Información.

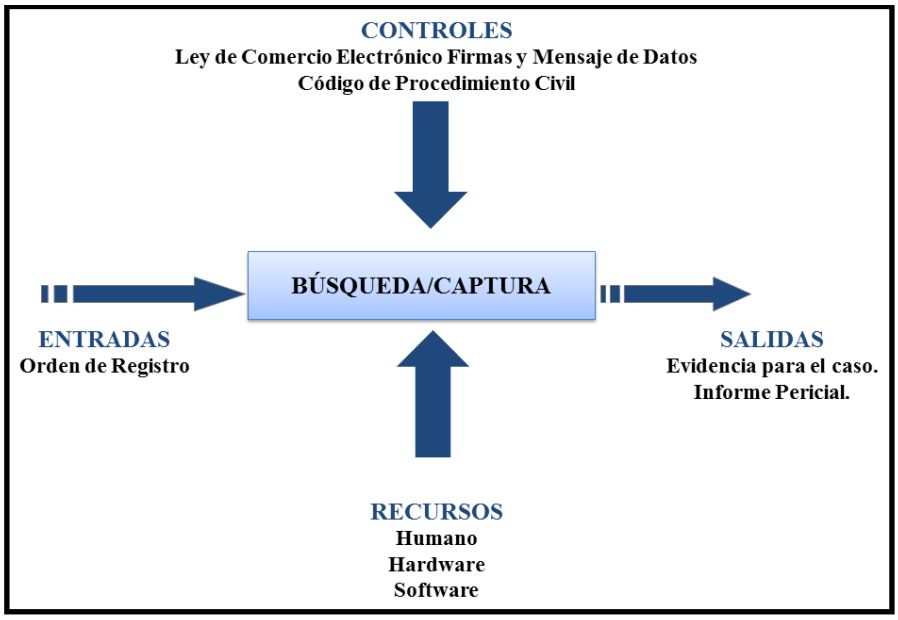


Figura #5.3 Proceso Búsqueda - Captura

Fuente: Autores

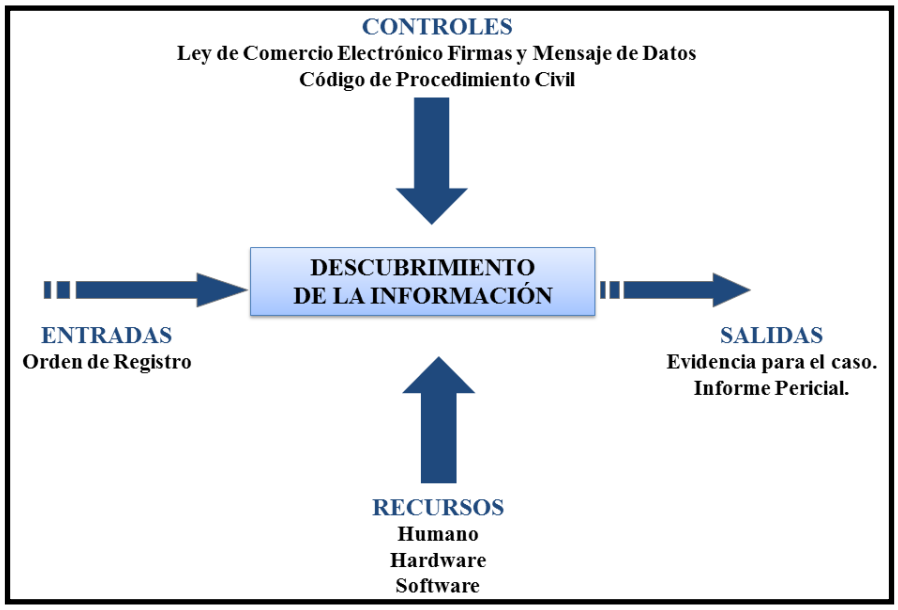


Figura 5.4 Proceso Descubrimiento de la Información

Fuente: Autores

Nivel 3: **Subprocesos de los Procesos:** Búsqueda – Captura y Descubrimiento de Información.

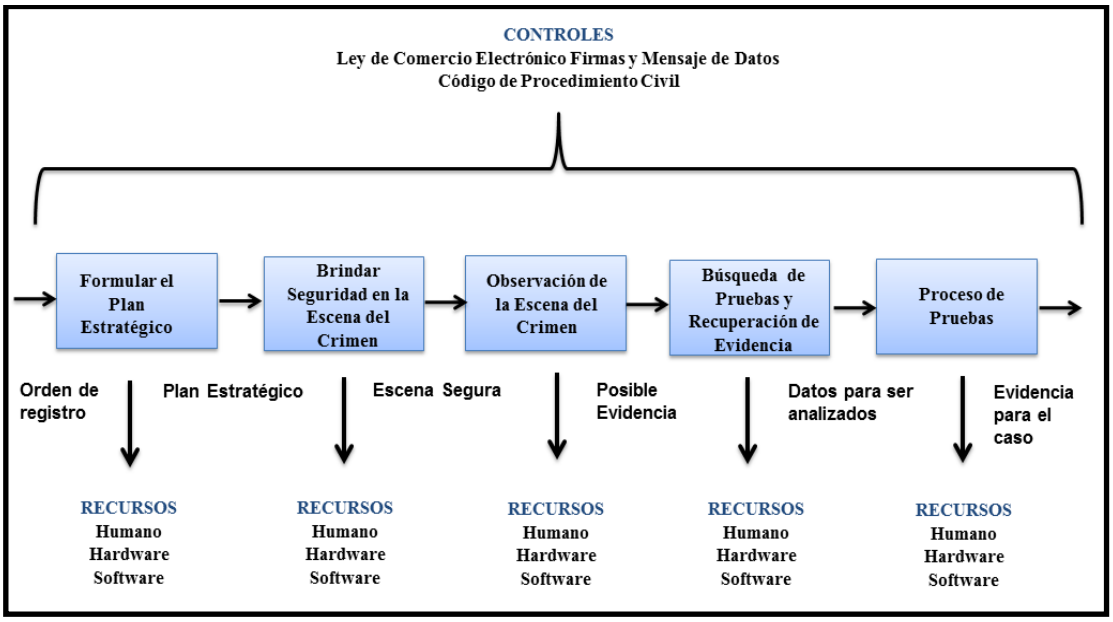


Figura 5.5 Subprocesos del Proceso Búsqueda - Captura

Fuente: Autores

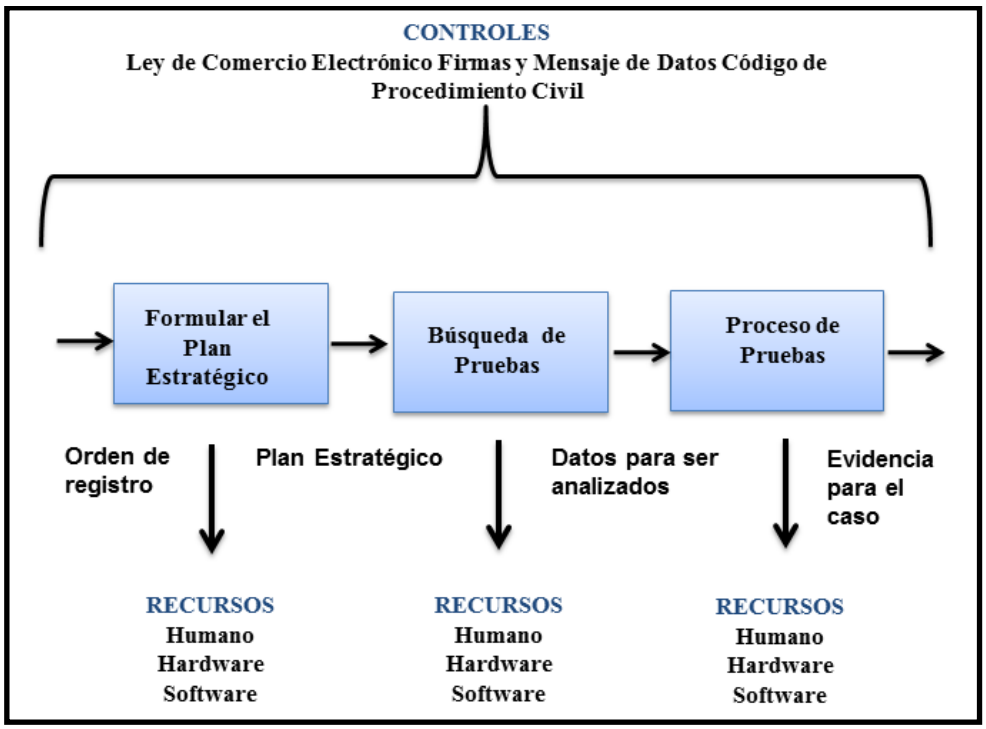


Figura 5.6 Subprocesos del Proceso Descubrimiento de la Información

Fuente: Autores

5.4.5 Las Reglas Básicas de Registro y Embargo

Registro e incautación consiste en la recuperación y el procesamiento de la evidencia en la escena donde se cometió el delito informático. Aunque en su mayoría sólo es bueno, el sentido común, las seis siguientes reglas deben estar siempre en la mente del investigador a lo largo de las etapas del trabajo de búsqueda y captura:

- No altere la evidencia original.

- No ejecutar programas en la computadora de la escena del delito informático (en especial el sistema operativo).

- No permita que un sospechoso interactúe en la computadora de la escena del delito informático.

- Siempre realice copias de seguridad de la computadora de la escena del delito informático, si un equipo está en la escena del delito informático, no lo apague hasta que todos los datos importantes en la memoria temporal se han salvado.

- Documentar todas las actividades de investigación.

- Respecto al almacenamiento de datos informáticos: si usted se siente cómodo allí, el equipo y los componentes se sientan cómodos allí.

En particular, estas reglas generales son útiles para el establecimiento de un protocolo por el cual la evidencia se reúne, manipula y almacena. Esto no sólo es esencial para el seguimiento y manejo de la evidencia que puedan derivarse de la escena del crimen informático.

Se explica con más detalle a continuación:

Regla 1: No Altere la Evidencia Original es una tarea fácil para evitar la alteración de hardware y software de prueba cuando la evidencia no está en uso. Sin embargo, cuando un equipo está ejecutando, se hace prácticamente imposible no cambiar su estado físico y lógico durante las interacciones. De hecho, incluso cuando un equipo se encuentra operativo desatendido podría ser ocupado escribiendo buffers de E / S, ejecución de trabajos de tiempo, y la realización de cualquier número de tareas de limpieza. Incluso los sistemas operativos simples pueden tener TSR (terminar y permanecer residente) la ejecución de programas en segundo plano. Siendo realistas, cualquier interacción del usuario con un equipo que está ejecutando puede causar cambios en el estado de dicho equipo. Siempre que un usuario haga una combinación de teclas en el teclado, los cambios se promulgan en la disposición de la computadora. Estos cambios pueden tener graves efectos sobre la prueba electrónica potencial.

Con el correr de hardware y software de sistemas, el gran cuidado debe ser tomado por el investigador para minimizar todas las interacciones, lo que disminuye la posibilidad de alteraciones en estos sistemas. Esto significa dos cosas:

- Durante un examen directo de una computadora de la escena del crimen, un disquete o CD de arranque se debe utilizar si el equipo se enciende (computadoras centrales, obviamente, no se podrá acceder de esta manera). Idealmente, estos exámenes deberían evitarse.

- En la medida de lo posible, las actividades forenses deben realizar copias de seguridad en el flujo de bits de una de las computadoras de la escena del crimen informático.

Al iniciar un equipo desde un disquete o CD, algunas de las actividades asociadas con el arranque del disco duro se eluden. A pesar de esta medida de seguridad, siempre es mejor interactuar con copias de seguridad de flujo de bits con los ordenadores de la escena del crimen informático para asegurarse de que la evidencia original no se altera. Desafortunadamente, con el fin de obtener una copia de seguridad de flujo de bits de un sistema, ese sistema tiene que ser interactuado con algún nivel. Además, algunos sistemas operativos son más adecuados que otros para

el trabajo forense. Linux es muy robusto, sistemas operativos POSIX estable y seguro, ofreciendo un apoyo significativo a los entornos informáticos diferentes. Debido a que Linux también pasa a ser capaz de encajar en uno o dos discos (dependiendo de la configuración), lo convierte en una herramienta de investigación excelente. Por ejemplo, un investigador podría desear para armar un disco de distribución de Linux con soporte para discos IDE y SCSI, redes, y algunas utilidades de archivos básicos del sistema. Si se necesita más capacidad, Linux también puede ser instalado para funcionar fuera de un cartucho ZIP o JAZZ.

Regla 2: No Ejecutar Programas en una Computadora de la Escena del Crimen en general, los equipos de la escena del crimen debe ser visto como piezas de museo: mira, pero no se toca. La ejecución de cualquier programa directamente en un ordenador podría causar daños a la prueba electrónica de valor, o, al menos, cambiar el estado de los recursos informáticos diversos. Debido a su capacidad de limpieza, un sistema operativo del ordenador tiene un enorme potencial de causar dichos daños, por ejemplo, valiosos datos temporales y caché podría ser "limpiado" de la existencia. Por esas raras excepciones cuando el software debe ser ejecutado en una computadora de la escena del crimen informático, la precaución extrema se debe utilizar y todas las actividades deben ser cuidadosamente documentadas.

Regla 3: No Permita que un Sospechoso Interactúe con una Computadora de la Escena de un Delito Informático evidencia electrónica desaparecerá rápidamente en manos de un sospechoso. Nunca debe haber alguna razón para que un sospechoso interactúe con una computadora de la escena del crimen informático o componente.

Regla 4: Siempre Realice Copias de Seguridad de la Escena del Crimen copias de seguridad de los ordenadores de la escena del crimen son esenciales para el trabajo forense: las actividades de investigación debe limitarse a las copias de seguridad para asegurar la integridad de la evidencia original. Un asunto de interés relacionado con las copias de seguridad de las computadoras, es la unidad RAM. Un investigador debe considerar o no que un delito operativo tiene una unidad o unidades de aplicación en la memoria residente. Obviamente, la copia de seguridad de flujo de bits de una unidad de disco requiere la interacción con el sistema operativo del equipo. Sin embargo, una unidad RAM podría ser un almacén de valor

incalculable de pruebas. Extrema precaución y el sentido común del investigador se deben utilizar aquí.

Regla 5: Documentar Todas las Actividades de Investigación es de suma importancia durante todo el trabajo de informática forense. Desde el momento que se abre un caso, hasta el momento en que se cierre la investigación implica que deben ser cuidadosamente registrados, junto con la fecha y hora. Una forma de implementar el registro, es que el investigador utiliza un ordenador portátil o notebook con un programa de hoja de cálculo simple. Con esto, si se está trabajando en el campo o el laboratorio de pruebas de la preservación, la documentación apropiada se puede cumplir. Por supuesto, ciertas precauciones en la configuración hay que tener: los datos de hoja de cálculo debe ser almacenado protegidos con contraseña, formato cifrado, y debe ser respaldada con una periodicidad razonable. Tenga en cuenta que el investigador debe tener hojas de cálculo separadas para los trabajos de campo y laboratorio. Una mejor alternativa a la utilización de hojas de cálculo sería el uso de software de gestión de caso.

Regla 6: El Almacenamiento de la Prueba Informática si bien es cierto que en general las pruebas de hardware y software pueden estar físicamente bien cuidados en entornos que también son muy cómodos para los seres humanos, el investigador debe tener cuidado de los campos electromagnéticos, la electricidad estática y el polvo para reducir la transmisión de cargas estáticas.

Un investigador a menudo se encuentra con situaciones en las que es imposible mantener la interacción con un equipo que se está ejecutando, pero estas interacciones, como se sabe, puede tener consecuencias destructivas sobre el estado original de la prueba informática. A pesar de que un investigador tiene toda la intención de evitar todas las interacciones destructivas con una computadora de la escena del crimen informático, la verdad del asunto es que muchas veces esto es imposible. Cuando se trata de la posibilidad de una unidad RAM, un investigador debe evaluar si la importancia de encontrar y realizar copias de seguridad en la unidad pesa más que los cambios destructivos que tales actividades causa a la computadora de la escena del crimen informático. Lo mejor que un investigador puede hacer es completamente documentar el estado original del ordenador de la

escena del crimen, junto con las medidas adoptadas durante las interacciones, y ser lo más cuidadoso y conservador como sea posible en estas interacciones.

Estas reglas ayudan a prevenir el mal manejo de la evidencia, y fomentar la documentación de las actividades de búsqueda y captura. En otras palabras, las reglas ayudan a asegurar una investigación de la cadena de custodia, lo cual es crítico para el éxito de cualquier caso.

5.4.6 Conceptos Básicos sobre la Recolección de Evidencia

Utilizando la Informática forense nos ocuparemos de la recolección y preservación de evidencia informática, así como el uso de esta prueba en procedimientos judiciales. Estas pruebas pueden ser tanto físicas como lógicas, ya que puede consistir en componentes de hardware y los medios de comunicación que contengan datos. El lado físico de la informática forense consiste en lo que se llama registro e incautación de evidencia informática.

El investigador en la escena de un delito informático, busca, y tiene en custodia hardware informático y medios de comunicación que están involucrados en el crimen. En contraste, en el lado lógico de la informática forense se ocupa de la extracción de datos en bruto de cualquier fuente de información relevante. Esto se conoce como el descubrimiento de información.

El investigador debe ser capaz de extraer información de las pruebas, pero sin provocar cambios en el estado original de esta evidencia. El estado original de la evidencia debe ser preservada a través de la investigación, desde el momento de que las pruebas se encuentran, al momento en que se cierra la investigación. La eficacia de las pruebas como la documentación objetiva, depende de lo bien que la evidencia ha sido preservada. A veces, la alteración de incluso unos pocos bits de datos puede tener consecuencias dramáticas en la investigación.

Una importante herramienta utilizada por los investigadores para preservar las pruebas, es la cadena de custodia. Que es el medio para darse cuenta de lo que se ha tocado en un determinado elemento de prueba, cuando lo tocó, y lo que hicieron a la

evidencia. Es una manera de demostrar que la evidencia no ha sido dañada o alterada. Como es de imaginar, los cambios en la cadena de custodia rápidamente pueden arruinar un caso.

5.4.7 Manejo de las Pruebas Electrónicas de la Escena del Crimen

Se deben tomar precauciones en la recolección, conservación y examen de las pruebas electrónicas.

Tratamiento de pruebas electrónicas en la escena del crimen consiste normalmente de los siguientes pasos:

- El reconocimiento y la identificación de las pruebas,
- Documentación de la escena del crimen informático,
- Obtención y preservación de la evidencia,
- Embalaje y transporte de las pruebas.

5.4.8 Las Herramientas Adecuadas para el Trabajo Adecuado

El investigador debe estar familiarizado con las buenas prácticas de administración de sistemas, poseer habilidades y conocimientos relevantes para la seguridad informática. Debe comprender las computadoras, sistemas operativos, bases de datos, y la función de las redes informáticas, y debe tener una comprensión básica de los diversos conceptos de trabajo en estas áreas. Además de habilidades y conocimientos, el investigador también debe tener la imaginación y habilidades deductivas para resolver los casos.

Las herramientas necesarias para investigar los delitos informáticos son relativamente sencillas. En primer lugar, en el lado del hardware, un laboratorio de conservación para las pruebas. Este es un entorno de alta seguridad (física y lógica) donde se procesa y se almacena la prueba informática. Se debe contar con instalaciones físicas para ayudar al investigador a realizar una variedad de tareas, así como experimentar e interactuar dentro de un rango de entornos informáticos. El

laboratorio pueden ser: Ethernet y Token Ring LAN, estaciones de trabajo Linux, otras estaciones de trabajo UNIX, PCs, sistemas de backup en cinta, lector de CD / sistemas de escritor, de alta capacidad de discos extraíbles, y una cantidad suficiente de medios nuevos en blanco.

En cuanto a las herramientas de software necesarias para la investigación de delitos informáticos, el software para ejecutar el laboratorio de preservación de pruebas es un requisito. Esto incluye sistemas operativos, bases de datos, los programas de archivo de datos para gestionar el backup en cinta y sistemas de CD de lectura / escritura, y un sistema de gestión de casos. El sistema de gestión de casos es un componente clave en el proceso de investigación, ya que proporciona al investigador un medio de almacenamiento de las notas del caso, la información sobre todos los involucrados y los elementos de una investigación determinada. Las preguntas sobre "quién", "qué", "dónde", "cuándo" y "cómo" se abordan en cada caso en los datos almacenados por el sistema de gestión de casos. Idealmente, estos datos se deben almacenar e interactuar de una manera segura: deben ser archivados mediante un cifrado fuerte, y el acceso a los datos del caso debe ser a través de un medio mediante la autenticación segura. Por supuesto, el sistema de gestión de casos debe proporcionar todas las características que se esperan de cualquier base de datos, tales como la capacidad para buscar, y generar estadísticas de los datos del caso. El sistema de gestión de casos es fundamental para mantener una fuerte cadena de custodia, y buena organización.

Una herramienta de software necesita ser discutido: Linux es un sistema operativo estable, seguro y eficiente. Bien apoyado en el procesador Intel, Sun, Alpha, PowerPC, y las plataformas de Motorolla, se adhiere Linux con el estándar POSIX, ofrece las discusiones a nivel de kernel y el soporte multiprocesador, cuenta con una base de software enorme, y, por supuesto, es libre. Tal vez la característica más importante de este sistema operativo es su alto nivel de calidad. Esto se debe a la filosofía de desarrollo que Linux emplea: cualquier persona que desee puede ofrecer mejoras y adiciones al kernel de Linux, pero todos los cambios están sujetos a la revisión amplia y crítica de la comunidad Linux. El resultado final es un programa en el que los usuarios de Linux mantienen una participación alta. Esto es especialmente importante para el esfuerzo de la informática forense, porque significa que Linux

ofrece una plataforma rica relativamente segura, robusta y sobre el cual trabajar. Tener Linux instalado en el laboratorio de preservación de pruebas, es una excelente manera de tener acceso a algunas utilidades de software de valor incalculable.

5.4.8.1 Herramientas Tecnológicas

De forma global**,** las herramientas tecnológicas que hay son muchas a nivel mundial. Su funcionalidad viene a ser la de ayudar al perito que realiza una investigación a encontrar mejores pruebas y de una forma más exacta y precisa, y que a la postre, sirva como evidencia clara para el debido proceso penal.

De esta forma, es posible decir que las herramientas informáticas son una base esencial para colaborar en el análisis de las evidencias obtenidas en un proceso forense. Sin embargo, el poderlas aprovechar al máximo y obtener la confiabilidad deseada de sus resultados tiene que ver mucho con la formación y el conocimiento con que cuente el investigador o perito que haga uso de ellas.

Pasaremos entonces a mencionar algunas de las herramientas que con frecuencia son utilizadas en procesos de informática forense, para adquirir un conocimiento general sobre ellas y su involucramiento en el proceso de investigación forense en informática.

ENCASE1. El software *EnCase* de la firma estadounidense *Guidance Software* es una de las herramientas clave de las fuerzas policiales que han empezado a utilizar técnicas de investigación cibernética. *EnCase* genera una imagen duplicada del disco duro que será utilizada como evidencia ante la justicia.

Este sistema incluye mecanismos que salvaguardan la integridad del contenido original del disco.

En el siguiente paso *EnCase* empieza a analizar la estructura de archivos del disco en busca de evidencias de actividades criminales. Esa herramienta penetra más allá del sistema operativo y busca en todos sitios donde encuentra datos. Esa búsqueda

incluye espacios vacíos, espacios no asignados y los archivos "*swap*" de Windows donde se almacenan documentos borrados y otras posibles pruebas.

FORENSIC TOOLKIT2: *ForensicToolkit de AccessData*(FTK) ofrece a los profesionales encargados de controlar el cumplimiento de la ley y a los profesionales de seguridad la capacidad de realizar exámenes forenses informatizados completos y exhaustivos. FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que se necesita.

FTK ha sido reconocida como la mejor herramienta forense para realiza análisis de correo electrónico.

Estos dos, son algunas de las muchas herramientas disponibles en el mercado. En ambos casos, son herramientas licenciadas y cuyos costos están entre los 600 y los 4000 o 5000 dólares. Aparte de estas aplicaciones, existen varios programas que no gozan de tanto reconocimiento a nivel mundial, llamados *software* de código abierto, que a pesar de no tener tanto renombre si han venido siendo tomadas en cuenta con el fin de que poco a poco tomen mayor posicionamiento en la práctica de informática forense.

Además, existen las herramientas a nivel de hardware que sirven también para bloquear discos duros, evitar que se copie información de ellos, entre otros, que colaboran paralelamente en este proceso.

Finalmente, cabe mencionar que existen en los mercados de países más desarrollados, computadores especializados para poder realizar investigaciones forenses.

5.4.8.2 Herramientas Físicas

5.4.8.2.1 Kit de Herramientas para el Procedimiento de la Escena del Crimen

Los investigadores deben tener en general las herramientas de procesamiento de la escena de la delincuencia. Los siguientes son elementos adicionales que pueden ser útiles en una escena del crimen electrónico:

5.4.8.2.2 Desmontaje y Herramientas de Eliminación

- Destornillador tipo hoja plana,
- Tuerca hexagonal,
- Alicates,
- Pequeñas pinzas,
- Destornilladores especializados (específico del fabricante, por ejemplo, Compaq, Macintosh),
- Destornilladores tipo estrella conductores de la tuerca,
- Cortador de alambre.

5.4.8.2.3 Envase y Transporte de Suministros

- Bolsas antiestáticas,
- Papel de burbujas antiestático,
- Cable,
- Bolsas de evidencia,
- Cinta de evidencia,
- Materiales de embalaje (evitar materiales que puedan producir electricidad estática, tales como espuma de polietileno o espuma plástica),
- Cinta de embalaje,
- Resistentes cajas de varios tamaños.

5.4.8.2.4 Otros Artículos

- Guantes,
- Carretilla de mano,
- Bandas de goma de gran tamaño,
- Lista de números de teléfono de contacto para obtener ayuda,
- Lupa,
- Papel de la impresora,
- Disco para incautación,
- Pequeñas linternas,
- Disquetes no utilizados (31 / 2 pulgadas y 51 / 4).

5.4.9 Como una Organización debe Resguardar la Información frente a un Delito Informático

Para asegurarse de que su organización puede reaccionar a un incidente de manera eficiente, asegúrese de que el personal sepa quién es el responsable de la seguridad cibernética y cómo llegar a ellos. Los pasos siguientes le ayudarán a documentar un incidente y ayudar a la Administración de Justicia en su investigación:

- Preservar el estado del equipo en el momento del incidente, haciendo una copia de seguridad de los registros, archivos dañados o alterados, y los archivos alterados por el intruso.

- Si el incidente está en curso, activar el software de auditoría y considerar la implementación de un programa de monitoreo del teclado si el sistema de registro de los permisos da la advertencia.

- Documento de las pérdidas sufridas por su organización como resultado del incidente. Estas podrían incluir:

    - Número estimado de horas de respuesta y recuperación,
    - Costo de la ayuda temporal,

- Costo de los equipos dañados,
- Valor de la pérdida de datos,
- Cantidad de créditos otorgados a clientes por las molestias,
- Pérdida de ingresos,
- Valor de los secretos comerciales.

- Comunicarse con la policía y

  - Proporcionar la documentación del incidente,
  - Compartir información sobre el intruso.

5.4.10 Mecanismos para que un Proveedor de Internet Divulgue Información

Se proporciona a los investigadores cinco mecanismos para obligar a un proveedor de servicios de Internet divulgar información que podría ser útil en una investigación de un hacker.

Los Mecanismos Muestran Requerimientos que se Describen a Continuación:

- Citaciones pueden ser utilizados por un investigador para obtener información sobre los abonados básicos de un proveedor de servicios de Internet, incluyendo "el nombre, dirección, número de teléfono o número de abonado o la identidad de otros, y tiempo de servicio de un abonado o los clientes de dicho servicio y los tipos de servicio al suscriptor o cliente utilizado.

- Citaciones también se puede utilizar para obtener abrir e-mails, pero sólo bajo ciertas condiciones relativas a la notificación al suscriptor. Una orden de registro es generalmente necesaria para abrir e-mails.

- Órdenes de la corte se puede obtener por los investigadores de los registros de cuentas y registros de transacciones. Estas órdenes están disponibles si el agente puede proporcionar "hechos articulables que muestran que hay

motivos razonables para creer que el contenido de una comunicación por cable o electrónico, o los registros u otra información buscada, son relevantes y pertinentes para una investigación penal en curso.

- Los investigadores que hayan obtenido una orden judicial pueden obtener el contenido completo de la cuenta de un abonado (excepto para abrir el correo electrónico almacenados con un proveedor de Internet por 180 días o menos, y correo de voz), si el pedido cumple con una disposición sobre notificación en el estatuto.

- Órdenes de cateo o una orden de estado equivalente puede ser utilizado para obtener el contenido completo de una cuenta, a excepción de buzón de voz en el almacenamiento electrónico.

5.4.11 Evidencia Potencial

5.4.11.1 Dispositivos Electrónicos

Pruebas electrónicas se pueden encontrar en muchos de los nuevos tipos de dispositivos electrónicos a disposición de los consumidores de hoy. Se muestra una amplia variedad de los tipos de dispositivos electrónicos comunes encontradas en la escena del crimen informático, se proporciona una descripción general de cada tipo de dispositivo, y se describen sus usos comunes.

Muchos dispositivos electrónicos contienen la memoria que requiere de energía continua para mantener la información, tal como una batería o corriente alterna. Los datos pueden ser perdidos fácilmente desconectando la fuente de energía o permitiendo que la batería se descargue.

Descripción: Un sistema informático normalmente consiste en una unidad principal, a veces llamado unidad de procesamiento central (CPU), almacenamiento de datos, dispositivos, un monitor, un teclado y un ratón. Puede ser independiente
o puede ser conectado a una red. Hay muchos tipos de sistemas informáticos, como ordenadores portátiles, ordenadores de sobremesa, los sistemas de torre, sistemas

montados en rack, minicomputadoras y mainframes. Los componentes adicionales incluyen módems, impresoras, escáneres, estaciones de acoplamiento y los dispositivos externos de almacenamiento de datos.

Por ejemplo, una computadora de escritorio es un sistema informático que consiste en, CPU y almacenamiento de datos, con un teclado externo y el ratón.

Principales usos: Para todo tipo de funciones de computación y almacenamiento de información, incluyendo procesamiento de textos, cálculos, comunicaciones y gráficos.

Evidencia potencial: La evidencia se encuentra más comúnmente en los archivos que se almacenan en los discos duros, dispositivos de almacenamiento y medios de comunicación.

5.4.11.1.1 Unidades de Procesamiento Central (CPU)

Descripción: A menudo llamado el "chip", que es un microprocesador ubicado dentro de la computadora. El microprocesador está ubicado en la caja principal del ordenador, en una placa de circuito impreso con otros dispositivos electrónicos.

Principales usos: Realiza todas las funciones aritméticas y lógicas del ordenador. Controla el funcionamiento de la computadora.

Evidencia Potencial: El dispositivo puede ser evidencia del robo de componentes, falsificación.

Figura 5.7 Unidades de Procesamiento Central (CPU)

Fuente: www.definicionabc.com

5.4.11.1.2 Memoria

Descripción: Extraíble placa de circuito dentro de la computadora.
La información almacenada aquí no suele ser retenida cuando el ordenador está apagado.

Principales usos: Información de usuario, de los programas y los datos mientras que la computadora está en funcionamiento.

Evidencia Potencial: El dispositivo puede ser evidencia del robo de componentes, falsificación.

Figura 5.8 Memoria
Fuente: www. markvision.com

5.4.11.1.3 Tarjetas Inteligentes

Descripción: Una tarjeta inteligente es un pequeño dispositivo manual que contiene un microprocesador que es capaz de almacenar, clave de cifrado o la información de autenticación (contraseña), certificado digital u otra información. Un escáner biométrico es un dispositivo conectado a un sistema informático que reconoce características físicas de un individuo (por ejemplo, huellas digitales, voz, retina).

Principales usos: Proporciona control de acceso a las computadoras, a los programas y a las funciones con una clave de cifrado.

Evidencia Potencial: Identificación / Autenticación de información de la tarjeta y el usuario, el nivel de acceso, configuraciones, permisos, y el propio dispositivo.

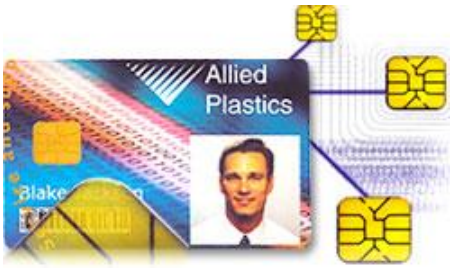


Figura 5.9 Tarjetas Inteligentes

Fuente: www. monografias.com

5.4.11.1.4 Contestadores Automáticos

Descripción: Un dispositivo electrónico que forma parte de un teléfono o conectado entre un teléfono y la línea telefónica.

Algunos modelos utilizan una cinta magnética o cintas, mientras que otros utilizan dispositivos electrónicos (digital) de registro del sistema.

Principales usos: Graba mensajes de voz de llamadas cuando el interlocutor está disponible o decide no contestar la llamada telefónica. Por lo general, tiene un mensaje en la parte de llamada antes de grabar el mensaje.

Dado que las baterías tienen una vida limitada, se pueden perder datos. Por lo tanto, el personal apropiado debe ser informado de que un dispositivo alimentado por baterías está en la necesidad de atención inmediata.

Evidencia Potencial: Contestadores puede almacenar mensajes de voz, y en algunos casos, el tiempo y la información actualizada sobre cuando se dejó el mensaje. También pueden contener otras grabaciones de voz.

Figura 5.10 Contestadores Automáticos

Fuente: www.puntotecno.cl

5.4.11.1.5 Cámaras Digitales

Descripción: La cámara, dispositivo de grabación digital de imágenes y video, con los medios de comunicación relacionados con el almacenamiento y hardware de conversión, capaz de transferir imágenes y vídeo a los medios informáticos.

Principales usos: Las cámaras digitales capturan imágenes y / o vídeo en un formato digital que es fácil transferir a los soportes informáticos para la visualización y / o edición.

Evidencia Potencial: Imágenes, hora y fecha. Cartuchos desmontables. Vídeo, sonido.

Figura 5.11 Cámaras Digitales
Fuente: www. markvision.com

5.4.11.1.6 Dispositivos Portátiles (Asistente Personal Digital (PDA), Organizadores Electrónicos)

Descripción: Un asistente personal digital (PDA) es un pequeño dispositivo que puede incluir teléfono / fax, buscapersonas, redes, y otras características. Se suele utilizar como un organizador personal. La computadora de mano se acerca a la funcionalidad de un sistema de escritorio informático. Algunos no contienen unidades de disco, pero pueden contener ranuras para tarjetas PC que puede contener un módem, disco duro, u otro tipo de dispositivo. Por lo general, incluyen la capacidad de sincronizar sus datos con otros sistemas informáticos, más comúnmente por una conexión en un soporte.

Principales usos: La informática portátil, almacenamiento y comunicaciones. Dispositivos capaces de almacenar información.

Dado que las baterías tienen una vida limitada, se pueden perder datos. Por lo tanto, el personal apropiado debe ser informado de que un dispositivo alimentado por baterías está en la necesidad de atención inmediata.

Evidencia Potencial:

- Libreta de direcciones,
- Agendas de citas,
- Documentos,
- E-mail,
- Escritura,
- Contraseña,
- Agenda,
- Los mensajes de texto,
- Los mensajes de voz.

Figura 5.12 PDA

Fuente: pspipod.wordpress.com

5.4.11.1.7 Discos Duros

Descripción: Una caja sellada que contiene discos rígidos (discos) recubierto con una sustancia capaz de almacenar información magnéticamente. Puede ser hallado en un PC, así como externamente en un caso independiente.

Principales usos: De almacenamiento de información, tales como programas, textos, imágenes, video, archivos multimedia, etc.

Evidencia Potencial: La evidencia se encuentra más comúnmente en los archivos que almacena.

Figura 5.13 Disco Duro
Fuente: www.compuchannel.net

5.4.11.1.8 Tarjetas de Memoria

Descripción: Los dispositivos amovibles de almacenamiento electrónico, que no pierden la información cuando la energía es retirado de la tarjeta. Incluso puede ser posible recuperar las imágenes borradas de las tarjetas de memoria.

La tarjeta de memoria puede almacenar mucha información. Utilizado en una variedad de dispositivos, incluyendo ordenadores, cámaras digitales, y PDAs. Ejemplos son tarjetas de memoria, tarjetas inteligentes, memoria flash, y tarjetas de memoria flash.

Usos principales: Proporciona, métodos para almacenar y transportar información.

Evidencia Potencial: La evidencia se encuentra más comúnmente en los archivos que almacena.

Figura 5.14 Tarjetas de Memoria
Fuente: www.markvision.com

5.4.11.1.9 Módems

Descripción: Los módems internos y externos (analógico, ADSL, RDSI, cable), módems inalámbricos, tarjetas de PC.

Principales usos: Un módem se utiliza para facilitar la comunicación electrónica, permite que el ordenador pueda acceder a otros ordenadores y / o redes a través de una línea telefónica, inalámbrica, u otras comunicaciones a mediano plazo.

Evidencia Potencial: El dispositivo en sí.

Figura 5.15 Modems
Fuente: www.infozilla.blogspot.com

5.4.11.1.10 Componentes de la Red

Red de área local o tarjeta de red. Estos componentes son indicativos de una computadora en la red.

Descripción: Las tarjetas de red, cables asociados. Tarjetas de red también puede ser inalámbrico.

Principales usos: Una tarjeta de red se utiliza para conectar computadoras. Tarjetas que permiten el intercambio de información y compartir los recursos.

Evidencia Potencial: El dispositivo en sí, MAC (Media Access Control) acceder a la dirección.

5.4.11.1.11 Enrutadores, Concentradores y Conmutadores.

Descripción: Estos dispositivos electrónicos están utilizados en los sistemas

informáticos en red. Routers, switches y hubs, proporcionan un medio en la conexión de ordenadores o redes diferentes.

Con frecuencia pueden ser reconocidos por la presencia de múltiples conexiones de los cables.

Principales usos: Equipo utilizado para distribuir y facilitar la distribución de datos a través de las redes.

Evidencia Potencial: Los propios dispositivos. Además, para los routers, los archivos de configuración.

Figura 5.16 Enrutadores
Fuente: www.portalnet.cl

5.4.11.1.12 Servidores

Descripción: Un servidor es una computadora que ofrece algún servicio para otros equipos conectados a él a través de una red. Cualquier ordenador, incluyendo un ordenador portátil, se puede configurar como un servidor.

Principales usos: Proporciona recursos compartidos, tales como, archivo de correo electrónico, almacenamiento, servicios de páginas Web y servicios de impresión para una red.

Evidencia Potencial:

- Las libretas de direcciones,
- Archivos de correo electrónico,
- Audio / archivos de vídeo,
- Imagen / archivos gráficos,

- Marcadores de Internet / favoritos,
- Archivos de base de datos,
- Hojas de cálculo. Documentos o archivos de texto.

Figura 5.17 Servidores

Fuente: www.drsis.pt

5.4.11.1.13 Cables de Red y Conectores

Descripción: Los cables de red puede ser de diferentes colores, grosores, y formas y tener conectores diferentes, dependiendo de los componentes que están conectados.

Principales usos: Conecta los componentes de una red informática.

Evidencia Potencial: Los propios dispositivos.

Figura 5.18 Cables de Red

Fuente: www.paraisoinformatico.com

5.4.11.1.14 Buscapersonas

Descripción: Un dispositivo de mano, electrónico portátil que puede contener evidencias volátiles (números de teléfono, correo de voz, e-mail).Los teléfonos celulares y asistentes personales digitales también pueden ser utilizados como

dispositivos de localización.

Principales usos: Para enviar y recibir mensajes electrónicos, numéricos (números de teléfono, etc) y alfanumérico (texto, a menudo incluyendo el correo electrónico).

Dado que las baterías tienen una vida limitada, se pueden perder datos. Por lo tanto, el personal apropiado debe ser informado de que un dispositivo alimentado por baterías está en la necesidad de atención inmediata.

Evidencia Potencial:

- Los mensajes de texto,
- E-mail,
- Los mensajes de voz,
- Los números de teléfono.

Figura 5.19 Buscapersonas
Fuente: www.meshbee.es

5.4.11.1.15 Impresoras

Descripción: Una variedad de sistemas de impresión, incluidos los térmicos, láser, de inyección de tinta, conectado a la computadora mediante un cable (de serie, bus paralelo, serie universal (USB), firewire) o acceder a través de un puerto de infrarrojos. Algunas impresoras contienen un búfer de memoria, lo que permite recibir y almacenar documentos de múltiples páginas al mismo tiempo que se imprimen. Algunos modelos también pueden contener un disco duro.

Principales usos: Texto impreso, imágenes, etc., desde el ordenador al papel.

Evidencia Potencial: Impresoras pueden mantener registros de uso, tiempo e información de la fecha, y, si está conectado a una red, pueden almacenar

información de la red. Además, las características únicas puede permitir la identificación de una impresora.

Figura 5.20 Impresora
Fuente: www.samsung.com

5.4.11.1.16 Dispositivos de Almacenamiento Extraíbles y Medios de Comunicación

Descripción: El medio utilizado para almacenar información de forma eléctrica, magnética o digital. (Por ejemplo, disquetes, CDs, DVDs, cartuchos, cintas).

Principales usos: Los dispositivos portátiles que pueden almacenar programas, textos, imágenes, video, archivos multimedia, etc.

Evidencia Potencial: La evidencia se encuentra más comúnmente en los archivos que almacena.

Figura 5.21 Cd
Fuente: www.electronica.practicopedia.lainformacion.com

5.4.11.1.17 Scanners

Descripción: Un dispositivo óptico conectado a una computadora, que pasa de un documento más allá de un dispositivo de exploración (o viceversa) y lo envía a la computadora como un archivo.

Principales usos: Convierte documentos, imágenes, etc., como archivos electrónicos, que se pueden ver, manipular, o transmitir en un ordenador.

Evidencia Potencial: El dispositivo en sí puede ser una prueba. La capacidad de análisis puede ayudar a demostrar las actividades ilegales (por ejemplo, la pornografía infantil, el fraude de cheques, la falsificación, el robo de identidad). Además, imperfecciones tales como marcas en el cristal puede permitir la identificación única de un escáner utilizado para procesar los documentos.

Figura 5.22 Scanner

Fuente: www.epson.com

5.4.11.1.18 Teléfonos

Descripción: Un teléfono, ya sea por sí mismo (como sucede con los teléfonos celulares), o una estación base remota (inalámbrico), o conectado directamente a la línea fija del sistema. Obtiene la energía de una batería interna, eléctricos plug-in, o directamente desde el sistema telefónico.

Principales usos: Comunicación de doble vía de un instrumento a otro, con líneas terrestres, la radio, los sistemas celulares, o una combinación. Los teléfonos son capaces de almacenar información.

Dado que las baterías tienen una vida limitada, se pueden perder datos. Por lo tanto, el personal apropiado debe ser informado de que un dispositivo alimentado por baterías está en la necesidad de atención inmediata.

Evidencia Potencial: Muchos teléfonos pueden almacenar nombres, números, y la información de identificación de llamadas. Además, algunos teléfonos celulares pueden almacenar información de la cita, correo electrónico y las páginas, y puede actuar como una grabadora de voz.

- Agendas de citas / Contraseña,
- Llamadas e información de identificación,
- Número de serie electrónico,
- Los mensajes de texto,
- E-mail,
- El correo de voz,
- Memo,
- Navegadores de Internet.

Figura 5.23 Teléfono

Fuente: www.panasonic.com

5.4.11.2 Varios Artículos Electrónicos

Hay muchos otros tipos de equipos electrónicos que son demasiado numerosas para ser mencionadas aquí que pueden ser encontrados en la escena del crimen informático. Sin embargo, hay muchos dispositivos no tradicionales que pueden ser una excelente fuente de información sobre las investigaciones y / o pruebas. Ejemplos: Skimmers de tarjetas de crédito, cajas de identificador de llamadas, grabadoras de audio y televisión en la web.

Las máquinas de fax, copiadoras y equipos multifunción pueden contar con dispositivos de almacenamiento interno y puede contener información de valor probatorio.

Recordatorio: La búsqueda de este tipo de pruebas puede requerir una orden de registro.

5.4.11.2.1 Copiadoras

Algunas fotocopiadoras mantienen los registros de acceso de usuario y la historia de las copias. Copiadoras con la exploración de una vez / Imprimir varias permite que los documentos que va a escanear una vez queden en la memoria, y luego imprimir más tarde.

Evidencia Potencial: Documentos, usuarios y registro de uso. Hora y fecha.

Figura 5.24 Copiadora
Fuente: www.samsung.com

5.4.11.2.2 Skimmers de Tarjetas de Crédito.

Skimmers de tarjetas de crédito se utilizan para leer la información contenida en la banda magnética de las tarjetas de plástico.

Evidencia Potencial: La información contenida; titular de la tarjeta en las pistas de la banda magnética incluye:

- Fecha de vencimiento, dirección de usuario,
- Número de tarjeta de crédito, nombre de usuario.

Figura 5.25 Skimmers de Tarjetas de Crédito
Fuente: hardsoftgeek.com.ar

5.4.11.2.3 Relojes Digitales

Hay varios tipos de relojes digitales disponibles que pueden funcionar como localizadores que almacenan mensajes digitales. Se puede almacenar más información, tales como libretas de direcciones, calendarios de cita, correo electrónico y notas. Algunos también tienen la capacidad de sincronizar información con las computadoras.

Evidencia Potencial:

- Libreta de direcciones,
- Notas,
- Agendas de citas,
- Los números de teléfono,
- E-mail.

Figura 5.26 Reloj Digital

Fuente: www.samsung.com

5.4.11.2.4 Máquinas de Fax

Facsímil (fax) máquinas pueden almacenar números de teléfono pre-programados y un historial de los documentos enviados y recibidos. Además, parte de la memoria contienen faxes de varias páginas a analizar y enviados en un momento posterior, así como permitir que los faxes entrantes queden en la memoria e imprimir después. Algunos pueden almacenar cientos de páginas de los faxes entrantes y / o salientes.

Evidencia Potencial:

- Documentos,
- Los números de teléfono,
- Cartucho de película,
- Envío / recepción de registro.

Figura 5.27 Máquina fax

Fuente: www.samsung.com

5.4.11.2.5 Sistemas de Posicionamiento Global (GPS)

Sistemas de posicionamiento global puede proporcionar información a través de la información de destino, puntos de paso y rutas. Algunos almacenan automáticamente los registros.

Evidencia Potencial:

- Punto de coordenadas o Camino,
- Destinos,
- La secuencia de los registros.

Figura 5.28 GPS

Fuente: www.alt1040.com

5.4.11.3 Archivos Creados por los Usuarios

Los archivos creados por los usuarios pueden contener pruebas importantes de las actividades de los criminales, tales como libretas de direcciones y archivos de base de datos que pueden resultar en una asociación delictuosa, imágenes fijas o en movimiento que puede ser una prueba de la actividad de pederastas, y las comunicaciones entre los delincuentes como por correo electrónico o cartas.

- Las libretas de direcciones,
- Archivos de correo electrónico,
- Audio / archivos de vídeo,
- Imagen / archivos gráficos,
- Marcadores de Internet / favoritos,
- Archivos de base de datos,
- Hojas de cálculo. Documentos o archivos de texto.

5.4.11.4 Archivos Protegidos de los Usuarios

Los usuarios tienen la oportunidad de ocultar pruebas en una variedad de formas.
Por ejemplo, pueden cifrar o proteger con contraseña los datos que sean importantes para ellos. También puede ocultar archivos en un disco duro o dentro de otros archivos o deliberadamente ocultar pruebas incriminatorias, archivos con un nombre inocuo.

- Los archivos comprimidos,
- Archivos cifrados. Archivos protegidos mediante contraseña,
- Ocultos los archivos. Esteganografía.

Las pruebas también se pueden encontrar en los archivos y otras áreas de datos creadas como una función de rutina del sistema operativo del ordenador. En muchos casos, el usuario no es consciente de que los datos se están escribiendo en estas áreas. Contraseñas, la actividad en Internet y los archivos temporales de copia de seguridad son ejemplos de datos que a menudo pueden ser recuperados y examinados.

Hay componentes de los archivos que pueden tener pruebas de valor, incluyendo la fecha y hora de creación, modificación, supresión, de acceso, nombre de usuario o de identificación, y los atributos de archivo. Incluso encendido el sistema puede modificar alguna de esta información.

- Archivos de copia de seguridad,
- Los archivos de registro,
- Los archivos de configuración,
- Cola de impresión de archivos,
- Cookies,
- Archivos de intercambio,
- Archivos ocultos,
- Los archivos del sistema,
- Archivos u historia,
- Los archivos temporales.

5.4.12 Informe Pericial

El informe pericial es el documento redactado por el perito informático, en el que se exponen las conclusiones obtenidas por el experto, tras la **investigación** de un caso de **delito informático.**

El Informe pericial debe incluir:

- Los datos del cliente,
- Los objetivos de la investigación,
- La declaración previa del **perito informático**, en la que se establecen los principios de profesionalidad, veracidad e independencia,
- Documentación sobre el proceso de adquisición de pruebas,
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación,
- Resultados de la **investigación informática** y conclusiones.

La elaboración del informe consta a su vez de tres fases:

- Fase de adquisición de las pruebas:
  Recogida de todos elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de los equipos informáticos se lleve a cabo con todas las garantías para las partes. La documentación del proceso de adquisición de las pruebas es una información que debe formar parte del **informe pericial**.

- Fase de la investigación:
  El perito informático realiza un análisis exhaustivo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

  Constarán en el informe todas las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

- Fase de elaboración de la memoria:
  Tras el minucioso estudio de la información almacenada en los dispositivos, intervenidos en la fase de adquisición de pruebas, el perito informático analiza los resultados obtenidos con el fin de extraer las conclusiones finales de la investigación.

  En esta última fase, el perito informático recopila la información que ha obtenido durante todo el proceso de investigación y redacta el informe o memoria que se presentará ante los Tribunales.

5.5 Consejos de Seguridad Informática

Relacionados con su Equipo Informático:

- **Actualice Regularmente su Sistema** operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. A veces, los sistemas operativos presentan fallos, que pueden ser aprovechados por delincuentes informáticos. Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de un hackers y la aparición de nuevos virus.

- **Instale un Antivirus** y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

- **Instale un Firewall** o Cortafuegos con el fin de restringir accesos no autorizados de Internet.

- Es recomendable tener instalado en su equipo algún tipo de **software anti-spyware**, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.

Relacionados con la Navegación en Internet y la Utilización del Correo Electrónico:

- **Utilice Contraseñas Seguras**, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

- **Navegue por Páginas web Seguras y de Confianza**. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:

    - Deben empezar por https:// en lugar de http.

    - En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

- **Sea Cuidadoso al Utilizar Programas de Acceso Remoto**. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la **seguridad de su sistema**.

- **Ponga Especial Atención en el Tratamiento de su Correo Electrónico**, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:

    - No abra mensajes de correo de remitentes desconocidos.

    - Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.

    - No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos como hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Estas cadenas de e-mails se suelen crear con el objetivo de captar las direcciones de correo de usuarios a los que

posteriormente se les enviarán mensajes con virus, phishing o todo tipo de spam.

- Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

5.6 Parte de la Resolución JB-2012-2148 de la Junta Bancaria

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar los siguientes cambios:

1. En el artículo 39, efectuar las siguientes reformas:

1.1 Sustituir el numeral 39.2, por el siguiente:

> **"39.2 Protección contra clonación de tarjetas**.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;"

1.2 Sustituir el numeral 39.6, por el siguiente:

> **"39.6 Protección al software e información del cajero automático.-** Disponer de un programa o sistema de protección contra intrusos (Antimalware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar

mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información.

En una situación de riesgo deben emitir alarmas a un centro de monitoreo dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;"

1.3 A continuación del numeral 39.6, incluir los siguientes y reenumerar los restantes:

"**39.7 Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.-** Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y remplazadas periódicamente;

39.8 Accesos físicos al interior de los cajeros automáticos.- Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras;

39.9 Reportes de nivel de seguridad de los cajeros- Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados;"

2. En el numeral 4.3.7. Sustituir el punto por punto y coma, e incluir los siguientes numerales:

4.3.8 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:

4.3.8.1 Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;

4.3.8.2 Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información;

4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;

4.3.8.4 La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y

deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado;

4.3.8.5 Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución;

4.3.8.6 Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;

4.3.8.7 Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas;

4.3.8.8 Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros.

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;

4.3.8.9 Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos;

4.3.8.10 Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

4.3.8.11 Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido.

Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura;

4.3.8.12 Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales

electrónicos y tarjetas;

4.3.8.13 Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas;

4.3.8.14 Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos;

4.3.8.15 Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero;

4.3.8.16 Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de

desarrollo y pruebas, ésta deberá ser enmascarada o codificada.

Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos.
Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada.

Esta información deberá conservarse por lo menos por doce (12) meses;

4.3.8.17 Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana;

4.3.8.18 Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales;

4.3.8.19 Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes;

4.3.8.20 Las instituciones del sistema financiero deberán ofrecer a los

clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;

4.3.8.21 Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;

4.3.8.22 Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos;

4.3.8.23 Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad;

4.3.8.24 Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad;

4.3.8.25 Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades;

4.3.9 Cajeros automáticos.- Con el objeto de garantizar la seguridad en las

transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente:

4.3.9.1 Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento;

4.3.9.2 La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece;

4.3.9.3 Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip;

4.3.9.4 Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores;

4.3.9.5 Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;

4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia y,

4.3.9.7 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es";

4.3.11 Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente:

4.3.11.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes;

4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia

y aplicando estándares vigentes y reconocidos a nivel internacional.

Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

4.3.11.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior;

4.3.11.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero;

4.3.11.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión;

4.3.11.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones;

4.3.11.7 Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica;

4.3.11.8 La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS);

4.3.11.9 La institución del sistema financiero debe implementar

mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres;

4.3.11.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one tim password), tener controles biométricos, entre otros;

4.3.11.11 En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas;

4.3.12 Banca móvil.- Las instituciones del sistema financiero que presten servicios a través de banca móvil deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11;

4.3.13 Sistemas de audio respuestas (IVR).- Las instituciones del sistema financiero que presten servicios a través de IVR deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11; y,

4.3.14 Corresponsales no bancarios.- Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8, 4.3.10 y 4.3.11."

5.7 Ejemplo de Informe Pericial

1. RESUMEN EJECUTIVO

A solicitud del XXXXXXXXXX, mi persona decidió tomar posición de perito informático forense para el caso de filtración de información privada y confidencial de la XXXXXXXXXX en el mes de XXXX a los 15 días del XXXX, donde se pudo obtener información de un Informe de auditoría interna emitido por los auditores de la XXXXXXXXXX y donde se describe quienes tuvieron acceso a la información transaccional de cheques en el sistema SAP que permitió obtener la información publicado por el diario XXXXX el día 6 de XXXX del XXXX, la cual se entrega a continuación:

- Se identifica y se analiza un informe emitido por el XXXXXXXXXX, gerente de auditoría interna con asunto de revisión de acceso transaccional a información de cheques y un **LOG** de evaluación de auditoría de seguridad donde están los accesos a los registros **FCHN – REGISTRO DE CHEQUES** del sistema **SAP** por los usuarios en el periodo del **1 de XXXXX del XXXX al 7 de XXXXX del XXXX**.

- En el informe se detallan 4 usuarios particulares que tuvieron acceso a los registros transaccionales FCHN – REGISTRO DE CHEQUES del sistema SAP y que fueron identificados del LOG de evaluación de auditoría de seguridad en el periodo ya dicho.

- Los usuarios descritos en el informe son:
  - ✓ XXXXXXXXXX**,**
    Jefe de Contabilidad.
  - ✓ XXXXXXXXXX**,**
    Analista de Tesorería.
  - ✓ XXXXXXXXXX**,**
    Analista Junior de Auditoría Interna.
  - ✓ XXXXXXXXXX**,**
    Analista de Tesorería.

- De los usuarios,

  - ✓ XXXXXXXXXX, en su rol de sus funciones no estaba autorizado al acceder a los registros transaccionales FCHN – REGISTRO DE CHEQUES, sin embargo tuvo un acceso a esta transacción el día 24 de XXXX del XXXX a las 12:56:24 PM.

  - ✓ XXXXXXXXXX, en su rol de sus funciones tenía autorización a acceder a los registros transaccionales FCHN – REGISTRO DE CHEQUES utilizándolo frecuentemente, sin embargo el Sr. XXXXXXXXXX venia teniendo un antecedente de divulgación de información confidencial por lo que su usuario XXXXX fue bloqueado el día 21 de XXXX del XXXX. El día 25 de XXXX del XXXX el Sr. XXXXXXXXXX se contacto con la mesa de ayuda de la XXXXXXXXXX el asunto de reactivación de su usuario, una vez que fue reactivado, ese mismo día el XXXXXXXXXX entro con su usuario XXXXXX a la transacción FCHN – REGISTRO DE CHEQUES del sistema SAP. El día 26 de XXXX del XXXX fue despedido.

  - ✓ XXXXXXXXXX, en su rol de sus funciones no está autorizado al acceder a los registros transaccionales FCHN – REGISTRO DE CHEQUES, sin embargo mediante una carta de alcance para la auditoria de controles de Tesorería (Ref. EC-F11-16) adjunta a este informe, tenía permiso a revisar movimientos de cheques específicos en los registros transaccionales FCHN – REGISTRO DE CHEQUES con fecha de acceso el día 25 de XXXX del XXXX a las horas 17:22:26 y 17:44:20.

  - ✓ XXXXXXXXXX, en su rol no estaba autorizado al acceder a los registros transaccionales FCHN – REGISTRO DE

CHEQUES, sin embargo fue promovida a las funciones que ejercía el Sr. XXXXXXXXXX de Analista de Tesorería teniendo ya autorización a acceder a los registros transaccionales FCHN – REGISTRO DE CHEQUES.

La Srta. XXXXXXXXXX solo tuvo acceso el día 26 de XXXX del XXXX a la 8:59:40 y hay un correo dirigido hacia mi persona por parte del Sr. XXXXXXXXXX explicando del porque la Srta. XXXXXXXXXX accedió a los registros transaccionales FCHN – REGISTRO DE CHEQUES.

- De los XXXXXXXXXX **y** XXXXXXXXXX que actualmente no trabajan en la XXXXXXXXXX y que se sospecha de divulgación de información confidencial de la XXXXXXXXXX según el informe de auditoría interno descrito en este informe, se realizó la pericia a sus correos electrónicos de la XXXXXXXXXX y a una Laptop con la que trabajaba el Sr. XXXXXXXXXX que también pertenece a la XXXXXXXXXX.

- De los correos del Sr. XXXXXXXXXX, en la carpeta enviados se encontró un correo en donde hay una imagen de una consulta a los registros transaccionales **FCHN – REGISTRO DE CHEQUES** parecido a la que fue publicada por el diario XXXXX el día 6 de XXXX del XXXX.

- De la laptop con la que trabajaba el Sr. XXXXXXXXXX, en su usuario XXXXX, en los temporales de internet, se encontró dos imágenes del cheque que se publicó en el diario XXXXX el día 6 de XXXX del XXXX.

- Como medio de preventiva, la información que está en la laptop HP descrito en este informe, los correos de los señores XXXXXXXXXX y XXXXXXXXXX y los archivo personales de estos señores, **van a**

estar firmados con un código numérico único llamado HASH para que no sea manipulado, y por su contenido de toda clase de información transaccionales confidencial, se encuentran en las instalaciones de la XXXXXXXXXX.

2. OBJETIVO DE LA PERICIA

Todos los actos periciales contenidos en este caso tienen por finalidad y objetivo demostrar de una forma científica y metodológica los siguientes puntos:

- Determinar en base a las evidencias, quien o quienes tuvieron acceso no permitido a los registros transaccionales **FCHN – REGISTRO DE CHEQUES en el sistema SAP**, obteniendo data confidencial de la compañía y que fue publicado por el **diario** XXXXXX **el día 6 de XXXX del XXXX**.

3. ANTECEDENTES PRELIMINARES

A continuación se entrega información del:

1. Informe hecho por el departamento de auditoría interna de la XXXXXXXXXX,
2. Un email dirigido hacia mi persona por parte del Sr. XXXXXXXXXX justificando el acceso de la Srta. XXXXXXXXXX a los registros transaccionales **FCHN – REGISTRO DE CHEQUES en el sistema SAP**,
3. Los respaldo de los correos en formato PST de los señores XXXXXXXXXX y XXXXXXXXXX,
4. Una laptop en el que trabajo el señor XXXXXXXXXX y que pertenece a la XXXXXXXXXX y donde están guardados los correos y archivos de los Señores XXXXXXXXXX y XXXXXXXXXX,

5. Una carpeta temporal de internet recuperado, que está dentro del usuario XXXXX en la laptop HP (descrito en este informe) que usaba para trabajar el XXXXXXXXXX.
6. Un respaldo de los archivos personales con que trabajaba el señor XXXXXXXXXX,
7. Una carta de alcance con referencia EC_F11_16,
8. y los registros de acceso de usuarios a la transacción FCHN – REGISTRO DE CHEQUES en el periodo del 1 de XXXX del XXXX al 7 de XXXX del XXXX.

Información Técnica de los archivos:

Por razones prácticas, solo se pondrán los archivos en donde hay evidencias de las transacciones FCHN – REGISTRO DE CHEQUES.

Nombre del Archivo	**Formato del Archivo**	**Fecha y hora en que fue creado el archivo**	**Software que se uso para el archivo**
1. Informe de auditoría - FINAL FIRMADO	PDF	15-Abrl-XXXX	Microsoft Office 2007
2. XXXXX Myo08	PST	19-Abril-XXXX	Microsoft Office Outlook
2. PST XXXXXX XXX	PST	19-Abril-XXXX	Microsoft Office Outlook
6. Carta de Alcance	PDF	22-Dic-XXXX	WorkCentre Pro
7. FCHN (Enero5-Febrero7)	XLS	07-Feb-XXXX	Microsoft Office Excel

Tabla 5.3

Fuente: Autores

Nombre de la	**Serial s/n**	**Sistema Operativo**	**Registro a nombre de:**	**Nombre del equipo**

compañía de la Laptop				
3. hp Compaq 6510b	CNU8291XSN	Microsoft Windows XP Pro	Dirección de Sistemas de infor. Desarrollo XXXXS.A XXXX 76460-OEM-0011903-00101	XXXX.XXX.XXXX.XXX.XXX

Tabla 5.4

Fuente: Autores

Nombre de la Carpetas	**Formato**	**Agregado**
Archivos temporales de Internet	ZIP	20-Abrl-XXX
XXXX	ZIP	20-Abrl-XXX
Respaldo XXXX 25-X-X	ZIP	20-Abrl-XXX

Tabla 5.5

Fuente: Autores

INFORMACIÓN DETALLADA DE CADA UNO DE LOS ARCHIVOS Y CARPETAS.

Archivo analizado: PST XXXXXX XXX.pdf

Captura de Pantalla: Cabe recalcar que estas dos captura de pantalla que se muestran a continuación, son archivo que contienen todos los correos de los Señores XXXXXXXXXX y XXXXXXXXXX.

Nombre:	PST XXXXXXXXXX
Extensión:	PST
Tamaño:	825,361 KB
Fecha de creación:	19-Abril-XXXX
MD5 Checksum:	9faab98bbae91e11da66e117502e6e2d

Figura 5.29 Archivo PST XXXXXXXXXX

Fuente: Autores

Nombre:	XXXXXXXXXX
Extensión:	PST
Tamaño:	2,529,617 KB
Fecha de creación:	19-Abril-XXXX
MD5 Checksum:	4e52f52aa92c645d28f5ddb111a7a123

Figura 5.30 Archivo PST XXXXXXXXXX

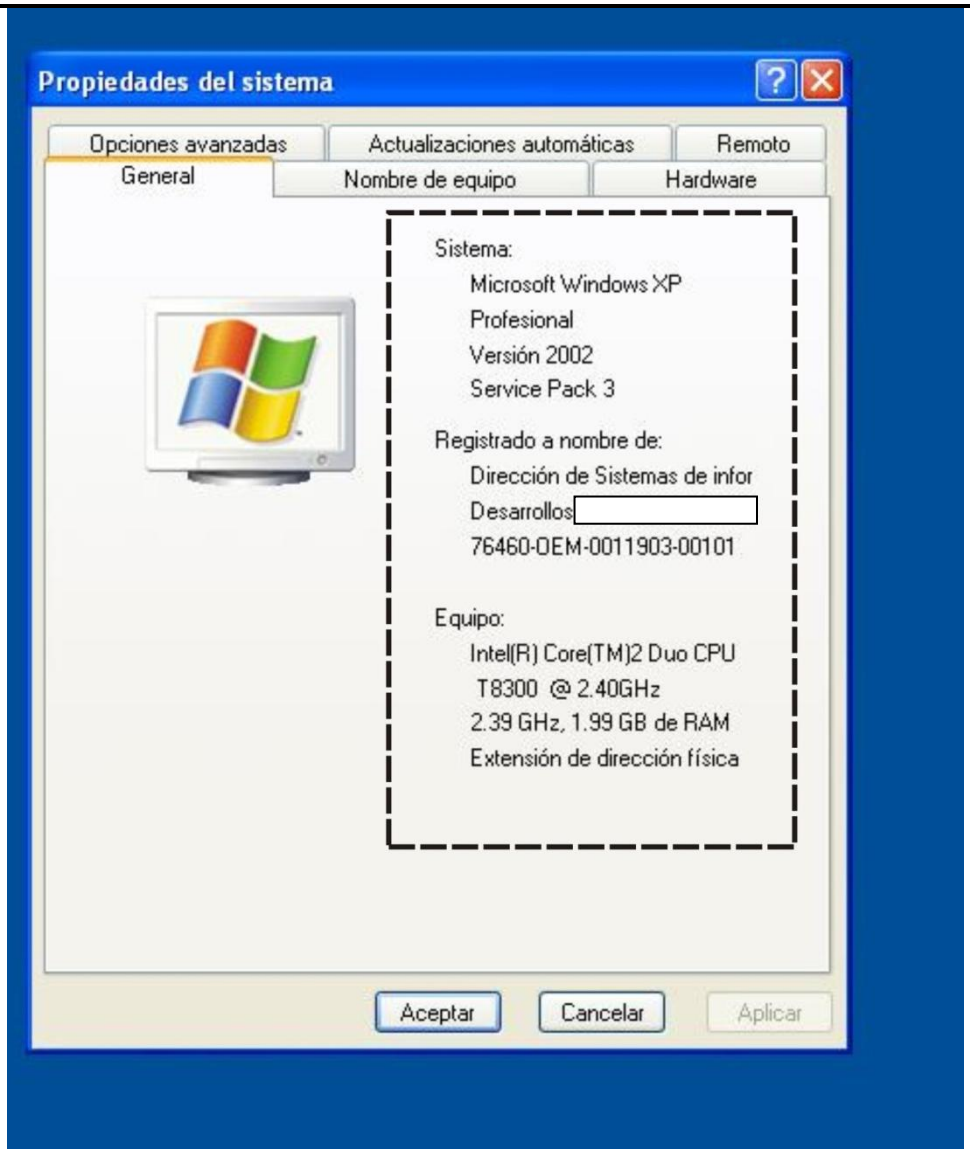
Fuente: Autores

Aclaración: *Estos archivo están Guardados en la laptop mencionado en el apartado "**Información Técnica de los archivos"** y que están en las instalaciones de la* XXXXXXXXXX. *Como medida de precaución, los archivos PST* XXXXXXXXXX *XXX.PST y* XXXXXXXXXX*Myo08.pst se los firmo con un valor numérico único (MD5 CheckSum) para que no haya modificaciones ni alteraciones y sea confiable la evidencia.*

Archivo analizado: Características de la laptop HP y que contienen los correos y archivos de los Señores XXXXXXXXXX y XXXXXXXXXX como evidencia.

Captura de Pantalla: Capturas de pantallas de la característica de la

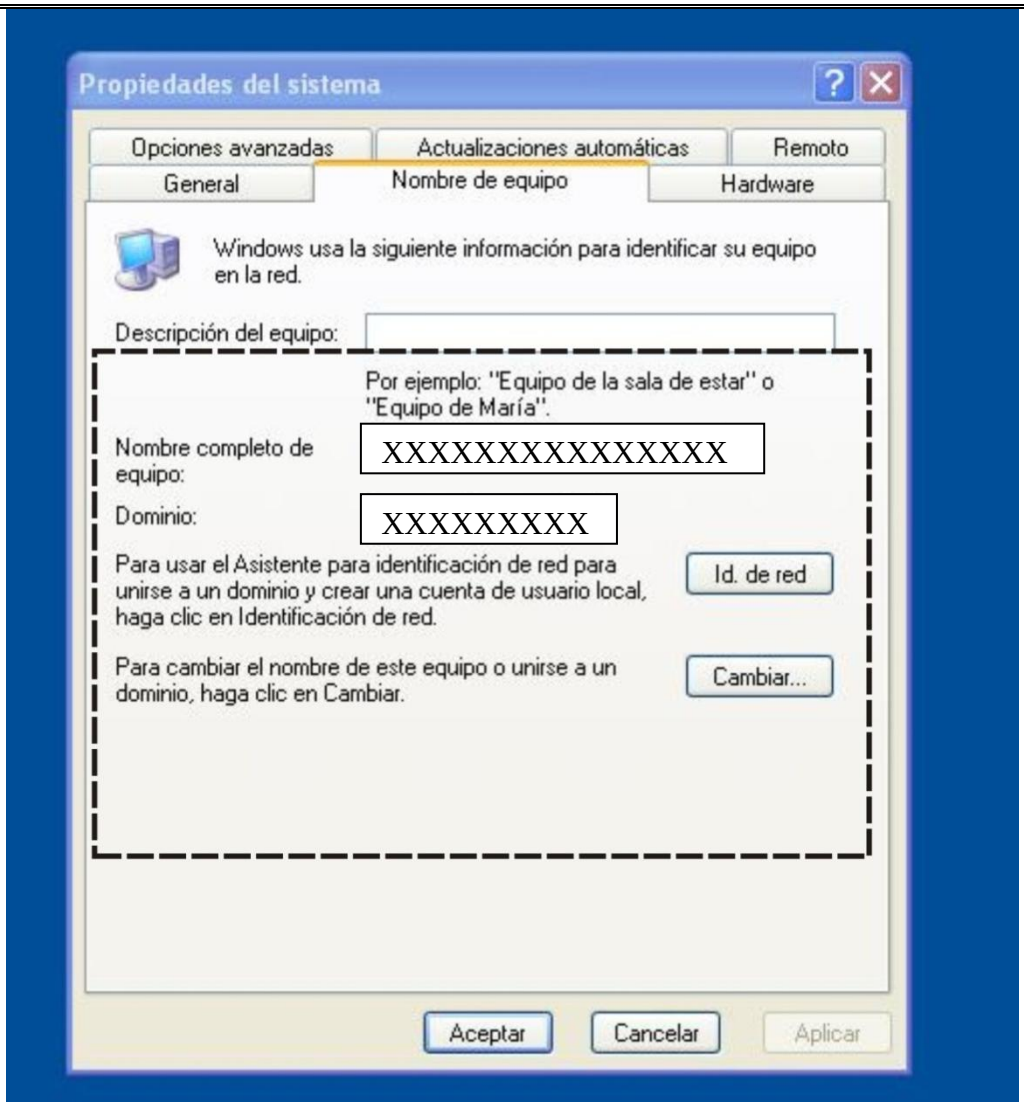
laptop HP y de los correos y archivos de los Señores XXXXXXXXXX y XXXXXXXXXX.



Nombre:	característica 1
Extensión:	JPG
Fecha de creación:	19-Abril-XXXX
MD5 Checksum:	72d365cb8f47214bbeaa862ddc4e52bc

Figura 5.31 Características

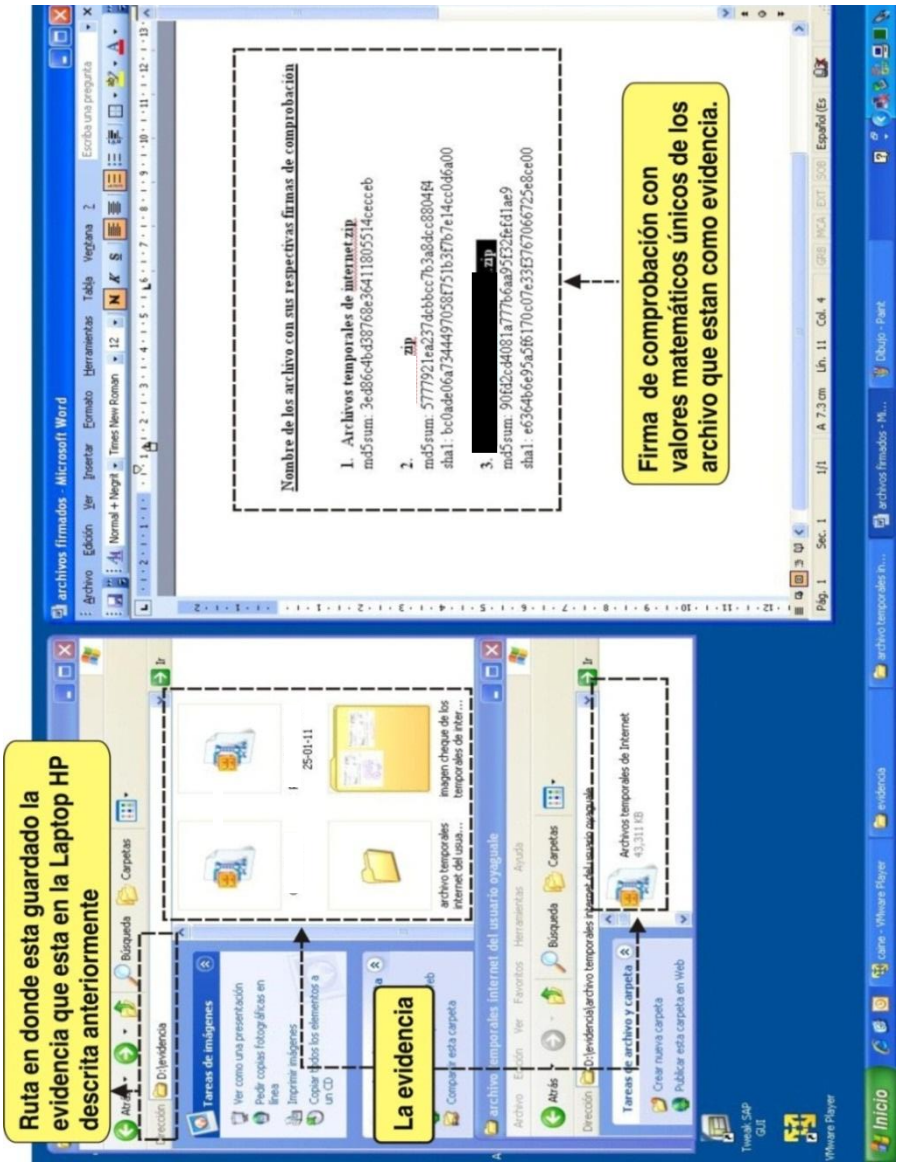
Fuente: Autores



Nombre:	características 2
Extensión:	JPG
Fecha de creación:	19-Abril-XXXX
MD5 Checksum:	cc4bb7866db9435fc87aea13e2661812

Figura 5.32 Características 2

Fuente: Autores



Nombre:	**Evidencia Firmados**
Extensión:	**JPG**
Fecha de	**20-Abril-XXXX**
Creación:	**e94c7cc0b155df9b1c5708202dbccf02**
MD5 Checksum:	

Figura 5.33 Evidencia Firmados

Fuente: Autores

Archivo analizado: Carta de alcance con referencia EC_F11_16

Captura de Pantalla: 3 Captura de pantalla de la carta de alcance

Nombre:	**Carta de Alcance**
Página	**1**
Extensión:	**PDF**
Fecha de creación:	**22-Dic XXX**
MD5 Checksum:	**f255e1963f4ea648b848e9250bd0e739**

Figura 5.34 Carta de Alcance

Fuente: Autores

Nombre;	**carta alcance 2**
Página:	**2**
Extensión:	**PDF**
Fecha de creación:	**22-Dic-XXX**
MD5 Checksum:	**f255e1963f4ea648b848e9250bd0e739**

Figura 5.35 Carta de Alcance 2

Fuente: Autores

Nombre;	**carta alcance 3**

Página:	**3**
Extensión:	**PDF**
Fecha de creación:	**22-Dic-XXX**
MD5 Checksum:	**f255e1963f4ea648b848e9250bd0e739**

Figura 5.36 Carta de Alcance 3

Fuente: Autores

Archivo analizado: Por cuestión de practicidad y porque son 8 hojas de tamaño A4, el archivo FCHN (Enero5-Febrero7).xls se adjunta en un CD que viene con el informe.

Captura de Pantalla: Captura de pantalla solo del archivo.

Nombre:	FCHN (Enero5-Febrero7)
Extensión:	XLS
Fecha de Creación:	7-Febrero-XXX
MD5 ChekSum:	bba086c03354642acc0df28d8da4f3b0

Figura 5.37 FCHN (Enero5-Febrero7)

Fuente: Autores

Archivo analizado: Correo del Sr. XXXXX detallando el motivo del acceso de la Srta. XXXXX al a los registros transaccionales **FCHN-REGISTROS DE CHEQUES**.

Captura de Pantalla: Captura de pantalla.

Nombre:	Correo-XXX
Extension:	JPG
Fecha del email:	25-Abril-XXX
MD5 ChekSum:	3074e473099b285e9f23f7fa745047c9

Figura 5.38 Correo-XXX

Fuente: Autores

4. PERICIA INFORMÁTICO FORENSE

La siguiente pericia está orientada a identificar alguna evidencia de filtración de información confidencial que haga referencia a lo publicado en el diario XXXX el día 6 de Febrero del XXX en los correos, archivos, de los señores XXXXX y XXXXX y una Laptop con la que trabajaba el Sr. XXXXX.

1er Paso.- Análisis de los archivos personales de los Señores XXXXX y XXXXX.

- Se analizó los archivos personales y no se encontró ningún tipo de evidencia que haga referencia a lo publicado en el diario XXXXX.

2do Paso.- Análisis de los correos electrónicos de la XXXXX de los Señores XXXXX y XXXXX.

- Se analizó los correos electrónicos de los Señores XXXXX y XXXXX.
- En la bandeja de entrada del correo del Sr. XXXXX se encontró un email con una imagen de una consulta de los registros de cheques que a continuación se detalla:

Nombre:	evidencia_correo_XXXX
Extensión:	JPG
MD5ChekSum:	1dadb33e713485122a069e392b251d34

Figura 5.39 Evidencia_correo_XXXX

Fuente: Autores

De las personas quien recibe el correo,

Nombre:	imagen_adjunto_correo
Extensión:	JPG
MD5ChekSum:	84af94f38ec8eb075b50c648ca17e399

Figura 5.40 Imagen_adjunto_correo

Fuente: Autores

De la imagen extraída del email encontrado,

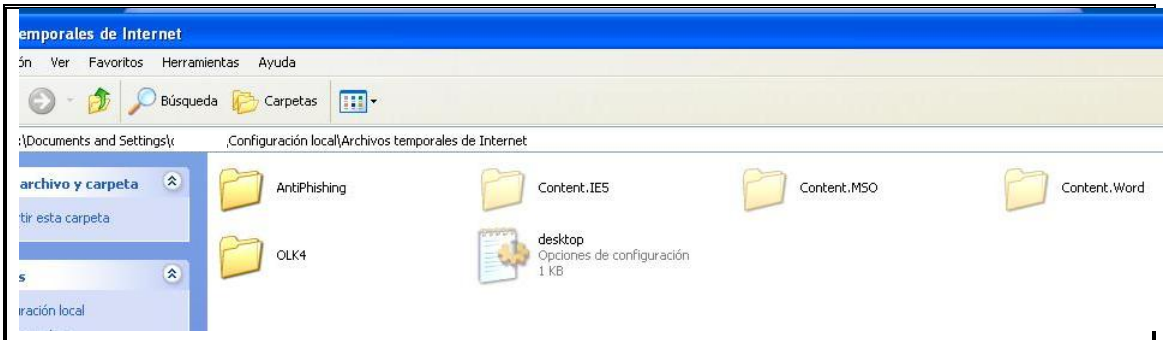
Nombre:	consulta_extraida_correo
Extensión:	JPG
MD5ChekSum de la imagen original:	a25c3ef26740aa87630292ad6f6b9b33

Figura 5.41 Consulta_extraida_correo

Fuente: Autores

4to Paso.- Análisis de los temporales de Internet de la laptop HP del usuario XXXX que usaba en el trabajo el Sr XXXXX.

En el análisis de los temporales,



Nombre:	archivo temporal Internet
Extensión:	JPG
MD5ChekSum de imagen Original:	1a0b7e51dd2c43e7f3c0548e44e20805

Aclaración: *Por cuestión practica, esta es una imagen recortada de la original.*

Figura 5.42 Archivo temporal Internet

Fuente: Autores

Se encuentra los siguientes archivos;

Nombre:	evidencia cheque desde XXXX
Extensión:	JPG
MD5ChekSum de la imagen original:	0f0bd4801d37a35d80e6f22ad7de5534

Aclaración: *La imagen es una ampliación de la original para mejor visualización.*

Figura 5.43 Evidencia cheque desde XXXX

Fuente: Autores

Nombre:	evidencia cheque desde XXXX
Extensión:	JPG
MD5ChekSum de la imagen original:	804331a5f427afc6fdc3fdceb837db9c

Figura 5.44 Evidencia cheque desde XXXX

Fuente: Autores

Archivos extraídos de los temporales de Internet mostrados en la imagen **evidencia cheque desde XXXX:**

Nombre:	ChequeXXXXXX
Extensión:	Jpg
Tamaño:	164 KB
Fecha de Creación:	4-Febrero-XXX
MD5ChecSum:	c19f0a23d72c8cf093ab398402eb8966

Figura 5.45 ChequeXXXXXX

Fuente: Autores

Archivos extraídos de los temporales de Internet mostrados en la imagen **evidencia cheque desde XXXXX** descrita en la página 27:

Nombre:	ChequeXXXXX
Extensión: jpg	Jpg
Tamaño: 33KB	33KB
Fecha de Creación:	4-Febrero-XXX
MD5ChecSum:	a5e08752fc4c7d0ceadddc9e152cd7ab

Figura 5.46 ChequeXXXXX

Fuente: Autores

5. CONCLUSIONES DE LA PERICIA

En honor a la verdad, la ética profesional y mi compromiso con la transparencia de la información en mis actuaciones como perito de cargo dentro de la indagación previa # 11-03-XXX (039-XXX), puedo certificar fehacientemente lo siguiente:

- Toda la información que contiene este informe técnico pericial, especialmente los correos electrónicos son científicamente elaborado y analizado con técnicas de informática forense.

- El informe de auditoría técnica analizado y descrito anteriormente, se comprueba en conjunto con un registro de LOG de auditoría de seguridad adjuntado a este informe, que el señor XXXXX tuvo acceso no autorizado a los registros FCHN-REGISTRO DE CHEQUES el día 24 de Enero del XXX a las 12:56:24 y que el Señor XXXXX también tuvo un acceso ya no autorizado a los registros dicho anteriormente el día 25 de Enero del XXX a las 9:39:39.

- Por una carta de alcance con # ref. EC_F11_16 y con fecha del 21 de Diciembre del XXX adjuntado a este informe, el Señor XXXXX por cuestión de trabajo tenía que acceder a los registros FCHN-REGISTRO DE CHEQUES el día 25 de Enero del XXX en las horas 18:11:55 – 17:22:26 – 17:44:20 y que por sus funciones de trabajo no está autorizado a acceder a estos, concluyendo que el señor XXXXX tiene justificación a ese acceso.

- La Srta. XXXXX también consta en el informe de auditoría interna que tuvo acceso el día 26 de Enero del XXX a las 8:59:40 a los registros FCHN-REGISTRO DE CHEQUES, sin embargo por un correo electrónico adjuntado a este informe enviado por el XXXXX hacia mi persona, explica el motivo de su acceso a esos registros, llegando a la conclusión de que la Srta. XXXXX no tiene que ver con

la filtración de información confidencial de la XXXXX publicada por el diario XXXXX.

- De los correos electrónicos del Señor XXXXX, en la carpeta de elementos enviados hay un email con una imagen adjunta de una consulta en los registros FCHN-REGISTRO DE CHEQUES del sistema XXX enviado por el Sr. XXXXX hacia XXXXX; XXXX; XXXXX y parecida a la que fue publicado en el diario XXXX el día 6 de Febrero del XXX. Cabe recalcar que el email tiene fecha 25 de Enero del XXX el día en que reactivo su usuario que fue bloqueado el día 21 de Enero del XXX y un día antes de que fuera despedido el 26 de enero del XXX.

- En la Laptop HP descrito anteriormente, dentro del usuario XXXXX y que pertenecía al señor XXXXX para el trabajo diario de sus funciones dentro de la XXXXXXX, se pudo extraer de los archivos temporales de internet de ese usuario XXXXX dos imágenes de un cheque que son idénticos a los que fue publicado por el diario XXXXX el día 6 de Febrero del XXX. Cabe recalcar que en las propiedades de esas imágenes tienen fecha de creación el día 4 de Febrero del XXX, dos días antes de que fueran publicadas por el diario XXXXX.

6. RESUMEN EJECUTIVO

Informática Forense

Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal

Sistemas Informáticos

Es el conjunto de partes interrelacionadas, hardware, software y de Recurso Humano. Un sistema informático típico emplea una computadora que usa dispositivos programables para capturar, almacenar y procesar datos. La computadora personal o PC, junto con la persona que lo maneja y los periféricos que los envuelven, resultan de por sí un ejemplo de un sistema informático.

SAP

SAP es una empresa Alemana, no un producto. Fue fundada en 1972 y significa: "Systeme, Anwendungen, Produkte" (Sistemas, Aplicaciones, Productos). El producto estrella de la compañía, al que todos simplemente llaman **SAP**, es su **ERP** (Enterprise Resource Planning), pudiéndose escuchar como nombre del mismo SAP.

Para entender que es **SAP**, se necesita saber lo que es un **ERP**, y la definición de este es que es "un sistema integrado de gestión de la organización".

Un sistema de estas características nos va a permitir administrar prácticamente todas las áreas de la organización: Producción, Ventas, Cuentas a Cobrar, Cuentas a Pagar, Contabilidad, Mantenimiento, Compras, Tesorería, Inventarios, Recursos Humanos, etc. Todos estos conjuntos de actividades están integrados en el aplicativo y cualquier actividad impacta en la otra automáticamente. Esto es lo que tiene la XXXXX.

Archivos Temporales

Es una carpeta "física" donde va guardando todo lo que vemos y no vemos al navegar por internet, todo lo que carga el navegador

(Internet Explorer, Firefox, etc.) desde el archivo .html (extensión de una página web) hasta los videos de youtube, mp3, imágenes, etc.

Firma Digital

Es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. La firma digital Consiste en un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento.

En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje. La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido.

Función HASH

En informática, **hash** se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*.

MD5 CheckSum

Valor numérico utilizado para verificar la integridad de un bloque de datos. El valor se calcula utilizando un procedimiento de suma de control. Una suma de control criptográfica incorpora información secreta en el proceso de suma de control de forma que no pueda reproducirse por quien no la conozca. Sirve para certificar que un archivo no sufrió cambios ni alteraciones desde su creación hasta su presentación.

Microsoft Outlook

Es un programa de organización ofimática y cliente de correo electrónico de Microsoft, y forma parte de la *suite Microsoft Office*.

PST

Son archivos de Microsoft Outlook que contienen correos electrónicos de una cuenta de usuario específica.

PDF

Portable Document Format (formato de documento portable) es el formato de archivos desarrollado por Adobe Systems. Esta tecnología ha tenido éxito estandarizando el formato de los documentos que se utilizan y transfieren en Internet. El PDF es como un formato de archivos universal.

Correo Electrónico

También conocido como e-mail, es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos) mediantes sistemas de comunicación electrónicos.

Ing. XXXXXX.
Perito Informático
XXXXXXXXXXX

Nota: Por ser un informe real no se mostrarán nombres ni fechas.

5.8 Ejemplo de Informe Técnico

INFORME TÉCNICO

A petición del Gerente General de la compañía XXXXXXXX S.A., Sr. Juan Piguave, el día martes 4 de abril del presente año, procedí a hacer un seguimiento de todas las actividades que realizare el Sr. Oliver Cant desde la computadora asignada para su trabajo diario dentro de las instalaciones de planta.

Dicho equipo, reúne las siguientes características:

- Pentium Celeron 2.4 Ghz
- Memoria RAM 256 Mb
- Mainboard
- Disco Duro 40 Gb

Es de indicar que en el equipo del Sr. Oliver Cant se encontraba el siguiente software instalado:

- Windows XP Professional(Sistema Operativo)
- Incredimal Mail(Gestor de Correos Electrónicos)
- Msn Messenger Live(Mensajería Instantánea)
- Microsoft Office 2003
- Skype 2.0 (Mensajería Instantánea)

Para llevar a cabo la petición se procedió a instalar el programa **OMNIQUAD DESKTOP SURVEILLANCE PERSONAL Versión 6.0.3**, que es un software de captura de pantallas y de pulsaciones en archivos .txt.

También se procedió a respaldar toda la información contenida en el disco duro, ya sean estos documentos, correos electrónicos, etc.

Todos estos datos fueron proporcionados al Sr. Juan Piguave en su respectivo

momento, encontrándose en ellos pruebas de que el Sr. Oliver Cant estaba cometiendo actos que afectaban directamente a la seguridad e imagen de la empresa; así como enviándose mails o correos electrónicos que afectaban la buena imagen de la compañía, así como, improperios en contra de sus representantes legales.

El día en que el Sr. Juan Piguave fue suspendido de sus labores en la empresa, por medio de la autoridad laboral que concurrió a las instalaciones de la misma, procedí a revisar la maquina en cuestión, me encontré con la novedad de que la contraseña de usuario había sido cambiada recientemente, por lo que tuvo que restablecerla desde el Administrador.

Volví a respaldar los documentos de la maquina y se encontró que había borrado parte de la información que existía. Con el programa **EASYRECOVERY PROFESSIONAL Versión 6.04**, que es un software que sirve para recuperar datos borrados de la computadora, busque dichos archivos, encontrándose con varios documentos borrados recientemente. Toda la información fue entregada al Sr. Juan Piguave.

Cabe indicar que todas las conversaciones encontradas fueron encontradas guardadas en la computadora, deduciendo que dichas conversaciones fueron grabadas por el mismo Sr. Cant.

Entre las conversaciones encontradas tenemos con:

- Sr. XXX XXX, Cliente de la Empresa.
- Sr. XXX XXX, ex Gerente de Comercialización de la Empresa.

También es importante añadir que la dirección de correo asignado al Sr. Cant, **ocant@xxx.com**, era de uso exclusivo de él, razón por la cual ningún otro usuario pudo haber enviado correos desde su dirección de e-mail. Las conversaciones en el Messenger Live desde la dirección **ocant@hotmail.com** y en el Skype con el user **Oliver Cant,** también son de exclusividad del Sr. Cant, ya que dichos servicios son de uso personal, y nadie a más de él conoce la clave. La clave de la computadora del Sr. Cant solo la conocía el y quien suscribe. Todos estos datos apuntan a que solo el

señor Cant tuvo dichas conversaciones con las personas antes mencionadas y que todos los datos restantes proporcionados fueron emitidos por el Sr. Cant.

Es todo cuanto se puede informar, en honor a la verdad.

f. Sr. Ing. XXX XXX XXX
Cédula de Ciudadanía No. 000000000
Jefe del Departamento de Sistemas
Procesadora XXXXXXX

Nota: Por ser un informe real no se mostrarán nombres originales.

5.9 Ejemplo de Delitos Informáticos

5.9.1 Phishing a Banco PICHINCHA

A menudo llegan a los correos mensajes supuestamente de los portales bancarios.

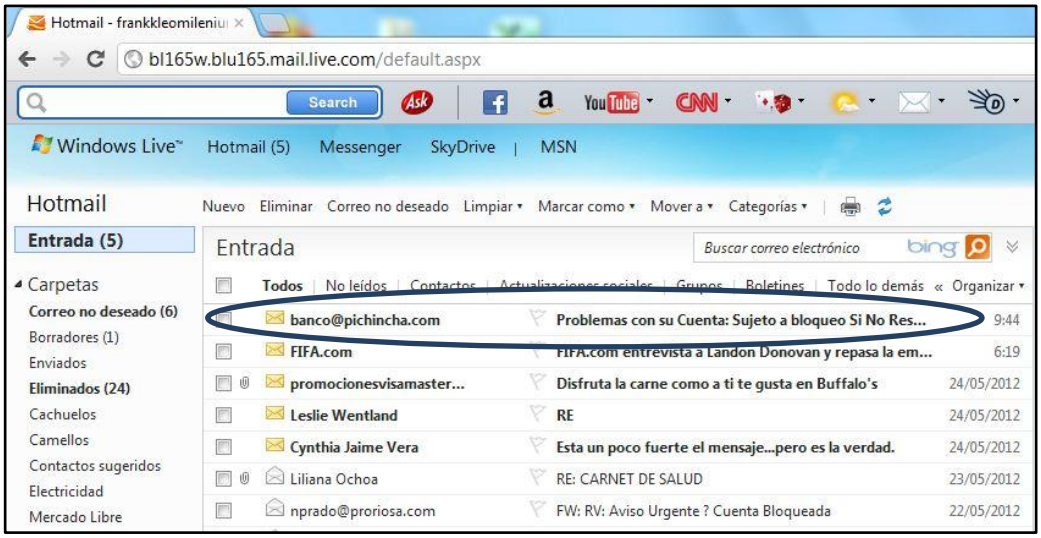


Figura 5.47 Phishing – Mensaje al Correo

Fuente: Autores

Como es costumbre se esgrime un tema para pescar al cliente incauto. En este caso el supuesto "bloqueo de la cuenta" e instan a "Activar Urgente". Por supuesto todo eso es falso, es el ardid para conseguir robar los datos bancarios de la víctima.

Figura 5.48 Phishing - Problema con su Cuenta

Fuente: Autores

En el mensaje indican que se debe ingresar un link para supuestamente desbloquear la cuenta.

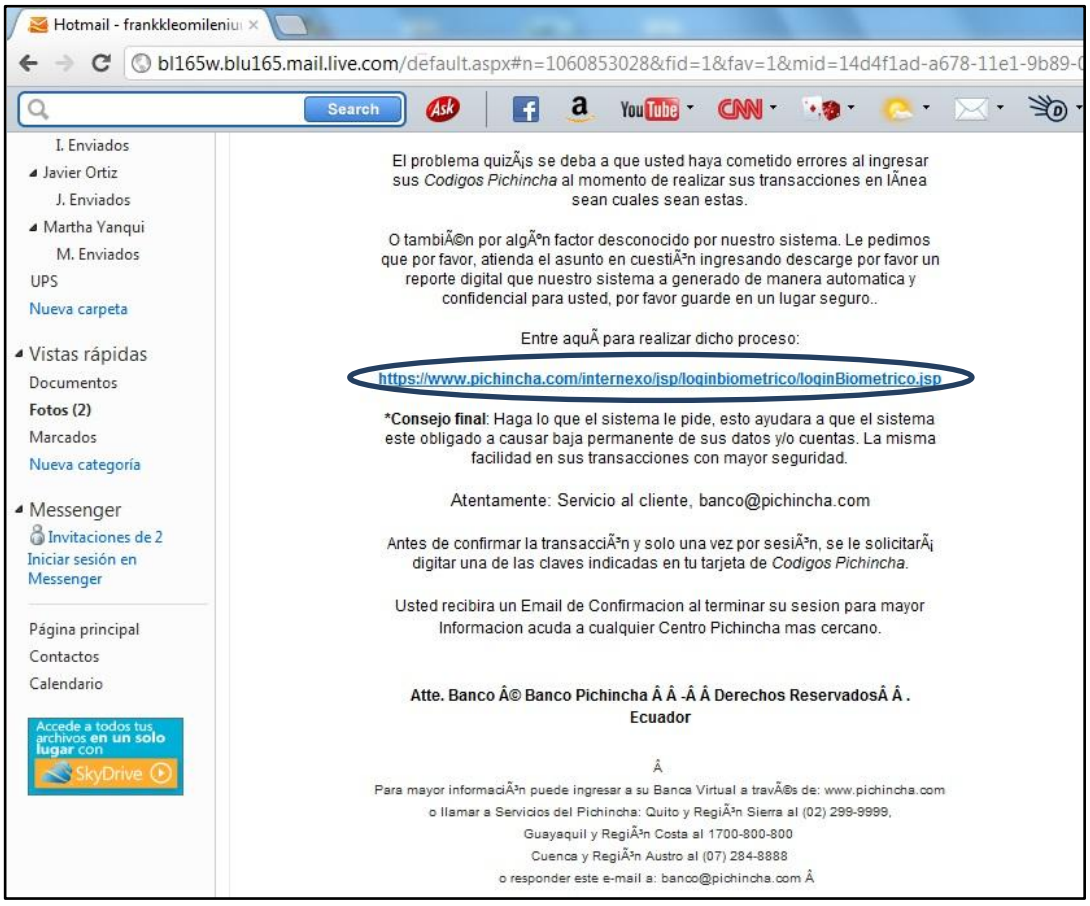


Figura 5.49 Phishing – Enlace a otra Página

Fuente: Autores

Al visitar ese sitio falso aparece una réplica de la página original, donde nos indica colocar nuestros datos.

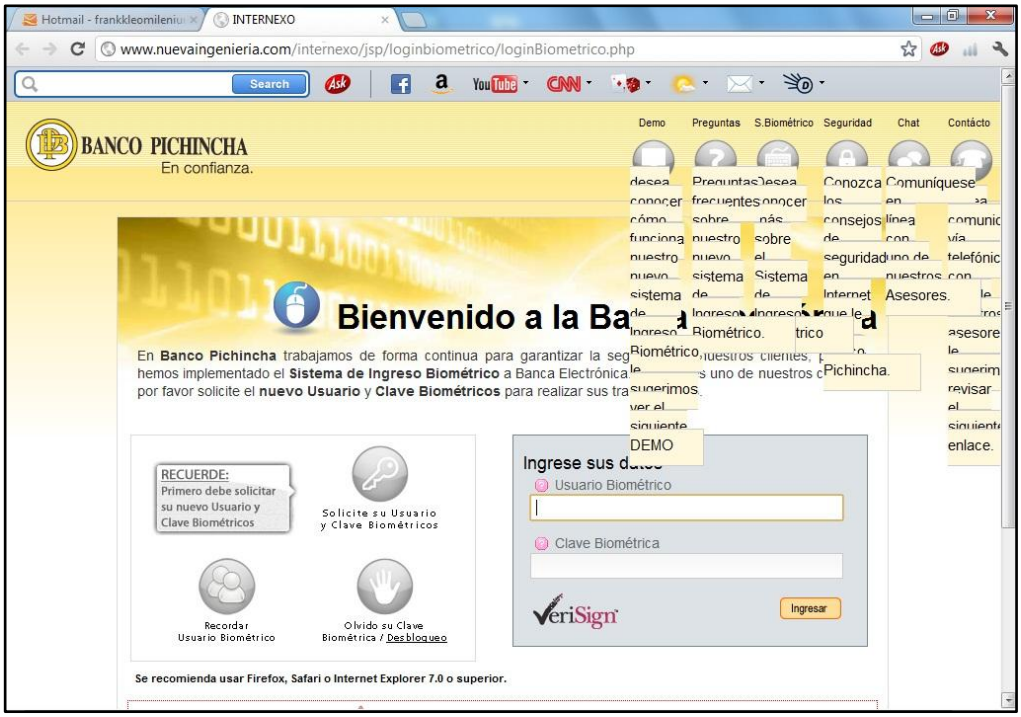


Figura 5.50 Phishing – Pedido de Datos

Fuente: Autores

Si se ingresan los datos, son enviados a los delincuentes mediante un formulario

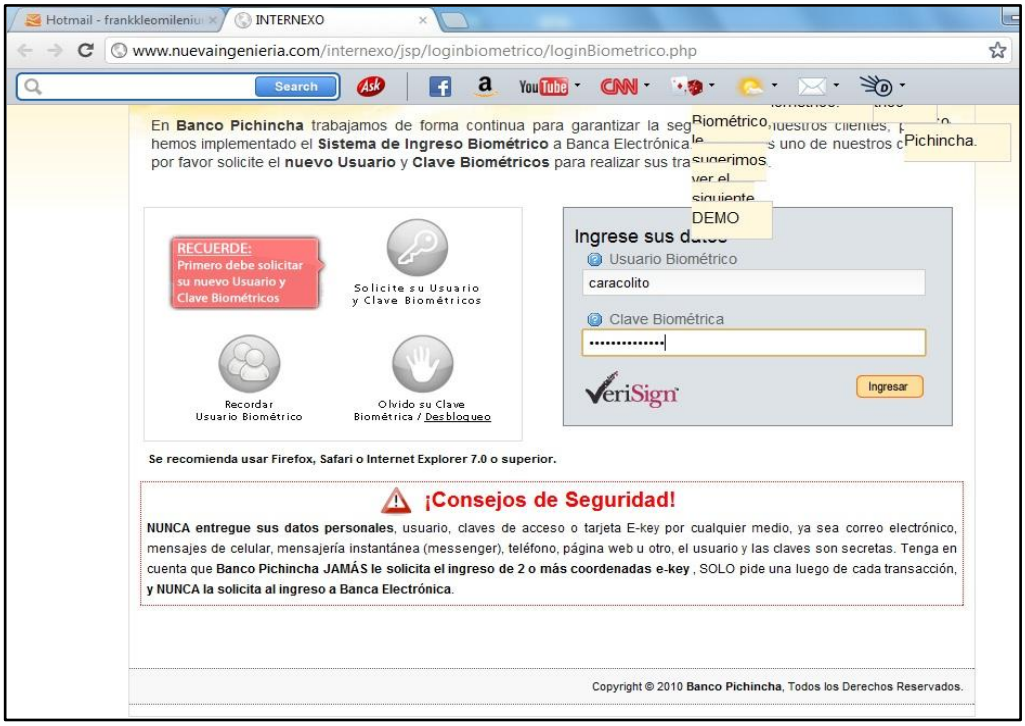


Figura 5.51 Phishing – Ingreso de Datos

Fuente: Autores

Y a nosotros se nos muestra el mensaje que nos indica que el sistema no está disponible por el momento.

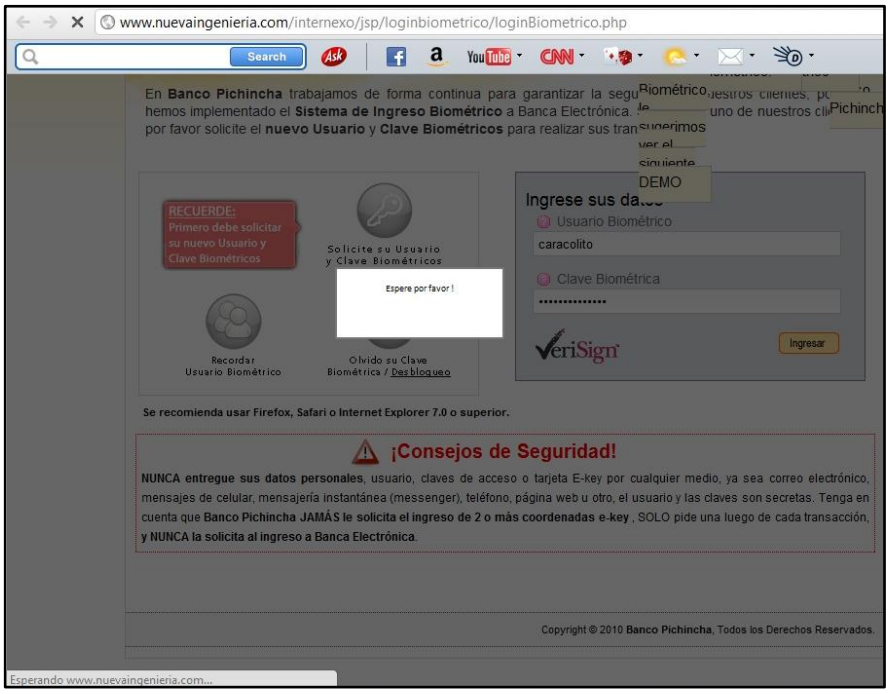


Figura 5.52 Phishing – Captura de Información

Fuente: Autores

Figura 5.53 Phishing – Mensaje de Error

Fuente: Autores

Para prevenir el Phishing:

- Utilice contraseñas fuertes con símbolos, números, mayúsculas y minúsculas y procure cambiarlas periódicamente.

- Memorice las contraseñas, no utilice la opción de almacenar que ofrece el navegador.

- Teclee siempre usted mismo la dirección de la página Web de la Entidad.

- Verifique que la dirección electrónica a la que está accediendo empieza con las siglas “https”, es decir, que además cuenta con una letra “s”.

- No siga enlaces que se encuentren en correos electrónicos aunque vengan de alguien conocido, mensajería instantánea o banners, que le podrían conducir a páginas falsas de la Entidad Financiera.

- Evite realizar transacciones en lugares de concesión pública a Internet.

- Valide siempre que en la parte superior o inferior del navegador aparezca el icono de un candado cerrado. De lo contrario no realice ninguna transacción.

- Al finalizar una transacción por Internet asegúrese de cerrar la sesión y borrar los archivos temporales.

- Recuerde que el **NINGÚN BANCO** lo contactará para solicitarle información confidencial como las contraseñas de sus cuentas, a través del teléfono, del correo electrónico o de cualquier otro medio.

- Actualice las opciones de seguridad de su computador y antivirus utilizando herramientas de seguridad adecuadas (antivirus, antispyware, firewall, etc.).

- Nunca preste su cuenta bancaria para recibir fondos cuyo origen usted desconoce, delincuentes utilizan este método para la transferencia de dinero de procedencia ilícita.

Aquí muestra el remitente **pichincha.com noreply@sonico.com**, nos podemos dar cuenta que el remitente no es el Banco del Pichinha.

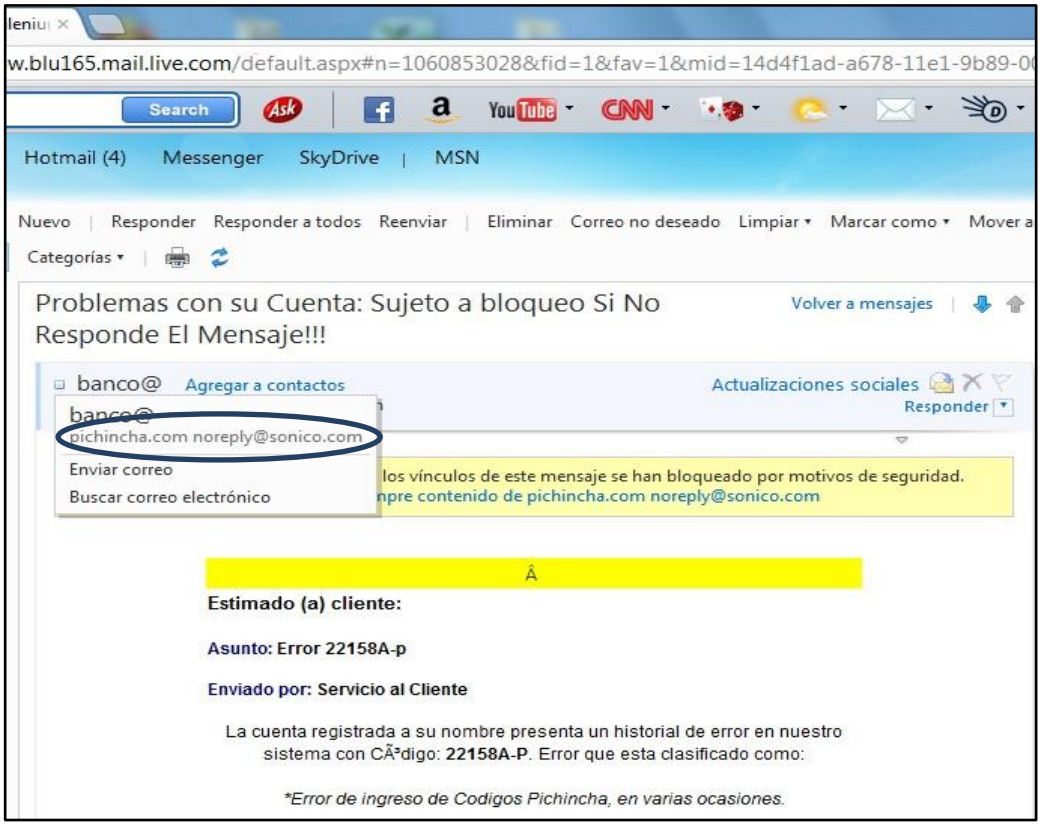


Figura 5.54 Phishing – Remitente Incorrecto

Fuente: Autores

Como se puede ver en la imagen, el enlace nos conduce a un sitio falso: www.nuevaingenieria.com/internexo/jsp/loginbiometrico/loginBiometrico.php

Figura 5.55 Phishing – Pagina Falsa

Fuente: Autores

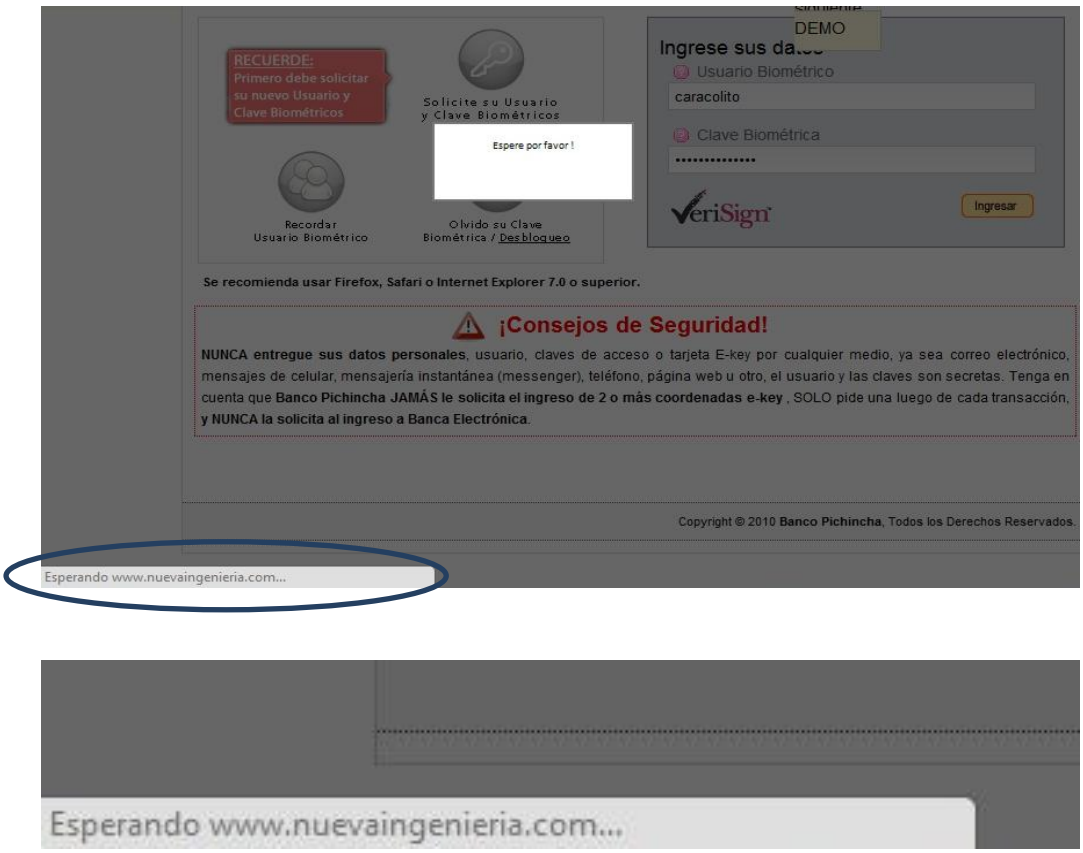


Figura 5.56 Phishing – Pagina Falsa 1

Fuente: Autores

5.9.2 Ejemplo de Scamming

Se envía al correo una carta donde supuestamente es acreedor de una suma de dinero.

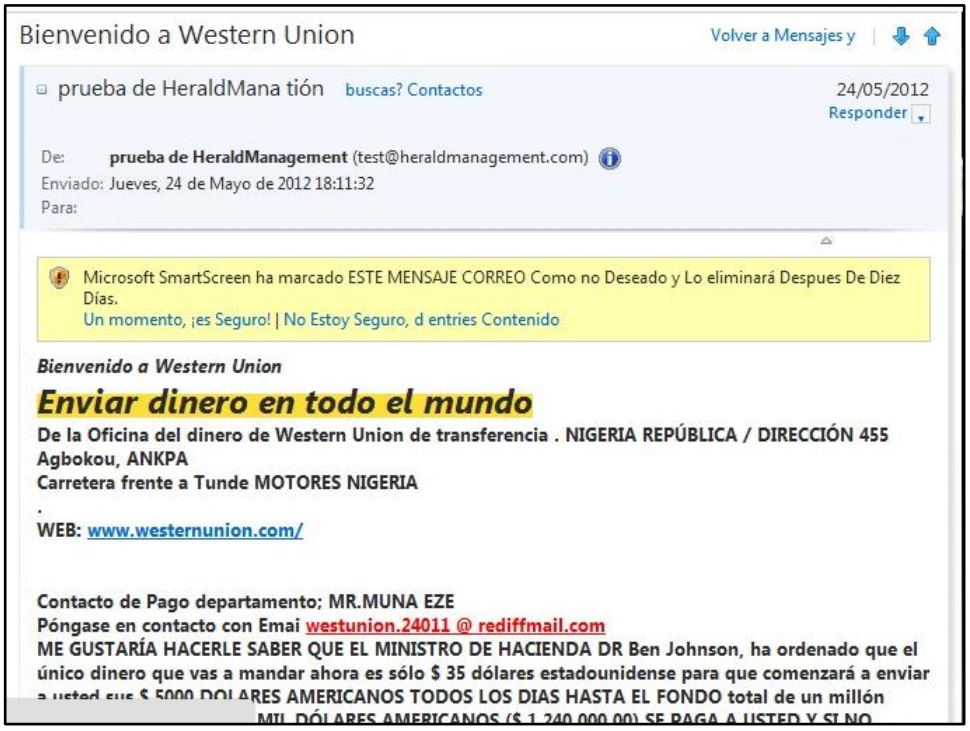


Figura 5.57 Scamming - Estafa

Fuente: Autores

Le indican que solo debe enviar una pequeña cantidad de dinero, para recibir una fuerte suma de dinero. Robando los datos de la persona y estafando ya que el dinero por parte de ellos nunca será dado.

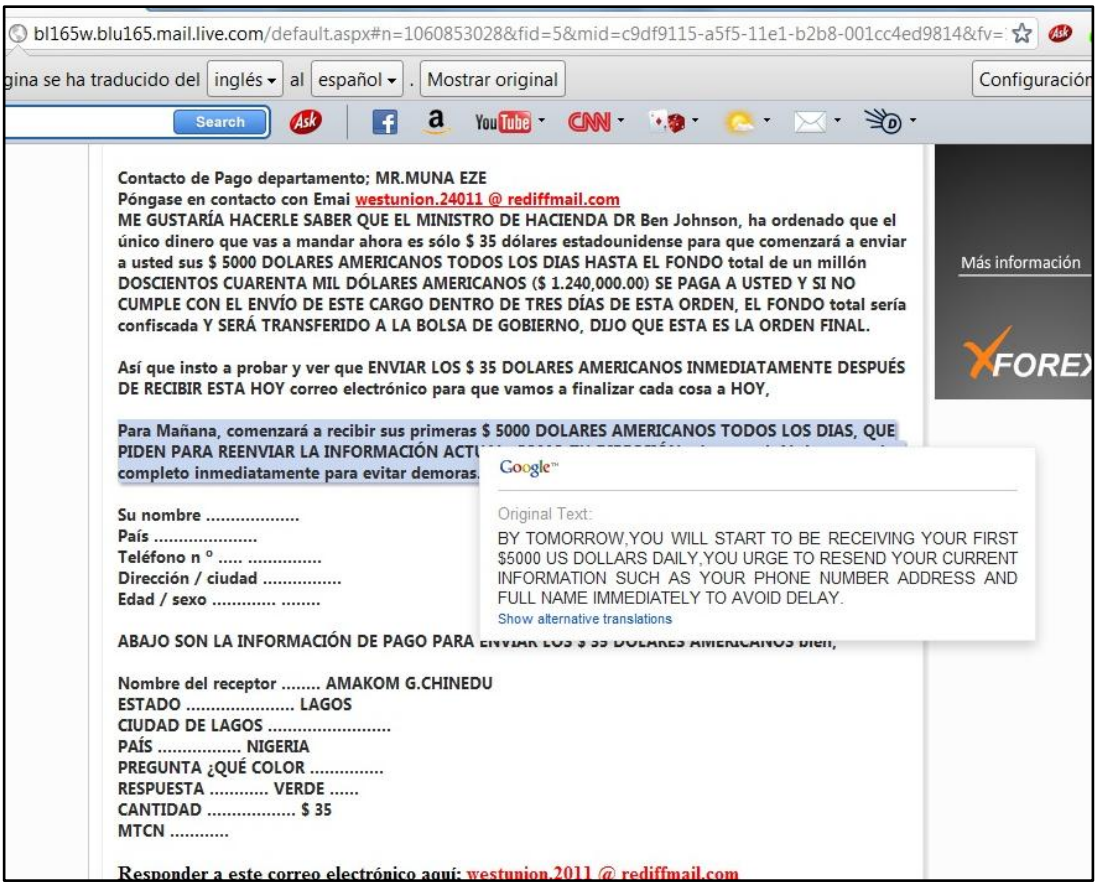


Figura 5.58 Scamming – Estafa 1

Fuente: Autores

Para prevenir el Skimming:

- Bloquee con su cuerpo y manos la visión sobre pantalla y teclado del cajero, para evitar que alguien vea su clave.

- Si el cajero no le entrega el dinero y el recibo indica que la operación fue exitosa, repórtelo de inmediato a la Oficina respectiva o al Call Center.

- Si el cajero presenta daños, no acepte ayuda de extraños, en ese caso cancele la operación y reporte el daño a algún funcionario de la Oficina más cercana.

- No utilice cajeros que presenten objetos extraños o alteraciones en su aspecto.

- Nunca introduzca su tarjeta en el cajero si éste se encuentra fuera de servicio.

- Si el cajero retiene su tarjeta, bloquéela inmediatamente por cualquiera de los canales dispuestos para tal fin.

- En caso de ser retenida su tarjeta haga caso omiso de avisos o mensajes para supuesto desbloqueo, donde le soliciten digitar su clave o lo remitan a teléfonos para reportarla.

CONCLUSIONES

El avance tecnológico y la necesidad de establecer procesos que permitan la indagación y resolución de delitos informáticos establece la importancia de contar con una nueva generación de profesionales que den respuesta a la creciente necesidad de la sociedad de contar con una buena Administración de Justicia, que sea capaz de brindar sustento y respaldo legal a cada una de los procesos planteados para de una forma más rápida y segura indagar y resolver los delitos informático.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Esta propuesta de la elaboración de un nuevo esquema para el procedimiento de indagación de los delitos informáticos espera generar un aporte a la Administración de Justicia en la Sociedad en materia de diferenciar los delitos informáticos del resto y de definir de una manera eficaz los procedimientos necesarios para la resolución a tiempo de los delitos informáticos.

Las organizaciones deben darse cuenta que su responsabilidad recae en la verificación de controles, evaluación de riesgos, minimizar las amenazas que presentan los delitos informáticos.

La presencia de delitos informáticos en las organizaciones no debe impedir que éstas se beneficien de todo lo que proveen las tecnologías de información, sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

La importancia científica de esta propuesta es la de aportar a la Administración de Justicia lineamientos que permitan planificar, motivar y gestionar rápidamente la indagación de delitos informáticos.

RECOMENDACIONES

En el Ecuador ya se ha manifestado la importancia de una investigación y sanción de los delitos informáticos, por lo que es preciso implementar y mejorar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los involucrados en la Administración de Justicia. Por lo que se recomienda lo siguiente:

- Poner en práctica los procesos y estrategias planteadas para la indagación de los delitos informáticos.

- Hacerle seguimiento a dichas estrategias.

- Que la administración de la Justicia se mantenga a la vanguardia en tecnologías, técnicas y procedimientos.

- Las Instituciones tecnológicas Superiores deben orientar su planificación y malla curricular a la especialización en el reconocimiento y formas de prevención de los Delitos informáticos.

Por otro lado es primordial propiciar la integración entre la administración de Justicia y los ciudadanos. Se necesite se eduque a la ciudadanía de los distintos tipos de delitos informáticos que existe, como la ley los protege y lo que necesitan hacer para hacer la denuncia respectiva, ya que para que inicie correctamente el proceso de indagación es primordial que las personas comuniquen inmediatamente cuando hayan sido blancos de delitos informáticos.

BIBLIOGRAFÍA

Direcciones Electrónicas

- **http://www.cibersociedad.net/archivo/articulo.php**

El sitio web pertenece al Observatorio para la CiberSociedad donde se publican trabajos e investigaciones sobre los diversos aspectos y corolarios socio-culturales que las nuevas tecnologías de la información están generando.

- **http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico**

Es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. La aplicación de mayor peso y a la que le debe su mayor fama hasta el momento ha sido la creación de enciclopedias colectivas.

- **http://es.wikipedia.org/wiki/Falsificaci%C3%B3n#cite_ref-0**

Es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. La aplicación de mayor peso y a la que le debe su mayor fama hasta el momento ha sido la creación de enciclopedias colectivas.

- **http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29**

Es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. La aplicación de mayor peso y a la que le debe su mayor fama hasta el momento ha sido la creación de enciclopedias colectivas.

- **http://www.hoy.com.ec/las-tics-ganan-popularidad-en-el-ecuador-405183.html**

Sitio web de diario ecuatoriano que presenta noticias locales e internacionales.

- **http://www.mundo-contact.com/enlinea_detalle.php?recordID=17990**

El portal Mundo Contact es el canal de comunicación especializado con la cobertura más grande en México y Latinoamérica, que vincula a los proveedores de productos y servicios con el público que busca soluciones para el desarrollo de sus estrategias tecnológicas y de mercado.

- **http://www.oei.es/tics.php**

Pagina Educativa de la Organización de Estados Iberoamericanos, muestra información de los diferentes sistemas educativos de los países miembros de la *OEI*. Noticias, legislación, publicaciones y evaluación.

- **http://www.pecert.gob.pe/index.php?option=com_content&view=article&id=50&Itemid=63&limitstart=9**

Portal Web del Sistema Nacional de Coordinación ante Incidentes Informáticos de Perú. Es un repositorio de la información referente a eventos en los cuales esté involucrada la seguridad en las redes, mediante la investigación, desarrollo, actualización de la información y difusión.

- **http://www.wikipedia.org/Tecnologías_de_la_información_y_la_comunicación.htm**

Es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. La aplicación de mayor peso y a la que le debe su mayor fama hasta el momento ha sido la creación de enciclopedias colectivas.

- **http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html**

El portal pertenece a la empresa española Recovery Labs que ha conseguido la certificación de su Sistema de Gestión de Calidad ISO 9001:2008 para sus servicios de recuperación de datos, borrado seguro y peritaje informático.

- **http://www.cert.org/tech_tips/FBI_investigates_crime.html#ccinv**

El Portal Web es el hogar del centro bien conocido de Coordinación del CERT, de la Universidad Carnegie Mellon de software, donde se estudian las vulnerabilidades de seguridad de Internet, la investigación a largo plazo cambios en el sistema de redes, y desarrollar la información y la formación para ayudar a mejorar la seguridad.

- **http://news.sequimpc.com/security/how-the-fbi-investigates-computer-crime/**

Portal Web de la empresa PC Sequim que ha estado en el negocio desde 2001, proporcionando de reparación de computadoras, soporte y actualizaciones a Sequim, Port Ángeles, y los residentes de los alrededores y las empresas.

- **http://www.justice.gov/criminal/cybercrime/usamay2001_2.htm**

Pagina del departamento de justicia de los estados unidos.

- **http://www.symantec.com/connect/articles/field-guide-part-three**

La Web de la empresa Symantec ayuda a las empresas y consumidores a proteger y administrar su información basada en el mundo.

- **http://www.symantec.com/connect/articles/field-guide-part-two**

La Web de la empresa Symantec ayuda a las empresas y consumidores a proteger y administrar su información basada en el mundo.

- **http://www.fbi.gov/about-us/lab/forensic-science communications/fsc/oct2000/computer.htm#Top of article**

FBI.gov es un sitio oficial del Gobierno Federal de los EE.UU., EE.UU. Departamento de Justicia

- **http://www.justice.gov/criminal/cybercrime/**

Pagina del departamento de justicia de los estados unidos.

- **http://www.us-cert.gov/cas/tips/**

Portal del US-CERT que es parte del Departamento de Seguridad Nacional .

- **http://news.sequimpc.com/security/how-the-fbi-investigates-computer-crime/**

PC Sequim ha estado en el negocio desde 2001, proporcionando de reparación de computadoras, soporte y actualizaciones a Sequim, Port Ángeles, y los residentes de los alrededores y las empresas.

- **http://www.ehow.com/way_5868687_steps-computer-crime-investigation.html**

EHow es su único recurso en línea para los desafíos de la vida. Los profesionales en cada campo se unen para ofrecer asesoramiento de expertos. Juntos, han creado una biblioteca en línea de los logros y está disponible para usted en cualquier momento y en cualquier lugar.

- **http://personal.telefonica.terra.es/web/pericali/noticias/del_informatico.htm**

Portal perteneciente a José Gabriel García Guirao - CRIMINÓLOGO - PERITO CALÍGRAFO FORENSE, donde aporta con artículos, trabajos, enlaces sobre delitos informáticos.

Libros

- Derecho Informático – Primera Edición, 2009
  Autor: Dr. Ricardo E. Nieves Galarza

- Fraude Online – Edición Informática64, 2011
  Autores: Dani Creus – Mikel Gastesi

ANEXOS

ANEXO A - MATRIZ DE INVOLUCRADOS EN LA ADMINISTRACIÓN DE JUSTICIA

Este anexo se aplica para indicar todas las personas que estarán involucradas en el proyecto, que recursos necesitan y el poder que ejercen sobre el mismo.
Se establece dentro del Capítulo 1 - pagina 42.

MATRIZ DE INVOLUCRADOS					
INVOLUCRADOS	**CARACTERÍSTICAS**	**INTERÉS/EXPECTATIVAS EN EL PROYECTO**	**RECURSOS**	**PODER**	**IMPLICACIONES**
Ciudadanos	Utilizan los servicios informáticos y son las víctimas de delitos informáticos.	Mejorar su seguridad electrónica. Que se resuelvan los delitos informáticos. Disminución de delitos informáticos. Disminuir la resistencia en el uso de los servicios informáticos.	Información.	Poder de convocatoria.	Denuncia de los delitos informáticos.
Ministerio Público	Institución encargada de responder con agilidad, solvencia, oportunidad y probidad la necesidad social de combatir a la delincuencia y a la corrupción.	Demostrar que la institución está cumpliendo con su labor. Mejorar su imagen.	Humano, Información Infraestructura.	Acusar a los presuntos infractores ante los jueces y tribunales competentes, e impulsar la acusación en la	Dirigir la investigación preprocesal y procesal penal con el apoyo de la Policía Judicial.

				sustanciación del juicio penal.	
Policía Judicial	Realiza la investigación de los delitos de acción pública y de instancia particular, bajo la dirección y control del Ministerio Público, a fin de reunir o asegurar los elementos de convicción y evitar la fuga u ocultamiento de los sospechosos.	Demostrar su responsabilidad social.	Humano, Información Infraestructura.	El conocimiento del Derecho Procesal Penal, los postulados básicos del Debido Proceso y los procedimientos técnicos jurídicos de investigación	Apoyar en la investigación preprocesal y procesal penal.

INVOLUCRADOS	CARACTERÍSTICAS	INTERÉS/EXPECTATIVAS EN EL PROYECTO	RECURSOS	PODER	IMPLICACIONES
Corte de Justicia	Administrar, vigilar y controlar con calidad, los recursos humanos, financieros, materiales y tecnológicos, para optimizar la administración de justicia y los servicios que ofrece en beneficio de los usuarios.	Colaborar con la sociedad y que se reconozcan como un referente positivo de la gestión pública.	Humano, Información Infraestructura.	Máximo tribunal de la función judicial. Aprobar nuestro proyecto del nuevo esquema de indagación de delitos informáticos.	Ejerce todas las atribuciones que le señalen la Constitución y las leyes.
Investigadores	Personas encargadas de indagar los delitos informáticos.	Colaborar con la sociedad.	Información.	Conocimiento de las TICS y de Delitos Informáticos. Utilizar nuestro proyecto del nuevo esquema de indagación de	Encontrar evidencia digital en el menor tiempo posible.

				delitos informáticos	
Estado	Velar por el bienestar de la sociedad.	Asegurar que disminuya los delitos informáticos y que continúe el desarrollo tecnológico del país.	Económico.	Máximo poder del país.	Garantizar mecanismos estadísticos y de juzgamiento.

\

ANEXO B - FODA DE LA ADMINISTRACION DE JUSTICIA

Este anexo estable todas las fortalezas, oportunidades, debilidades y amenazas de la Administración de Justicia, que es uno de los involucrados en el proyecto. Se establece en el Capitulo 1 - página 42

		OPORTUNIDADES		AMENAZAS
		1 Autonomía frente al resto de administraciones públicas. 2 Crecimiento constante de la tecnología.		1 Individuos que no tienen conocimientos informáticos básicos son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito. 2 Falta de conocimiento o interés de la sociedad. 3 La mayoría de los datos probatorios son intangibles y transitorios.
		ESTRATEGIA FO		**ESTRATEGIA FA**
FORTALEZA	1 Se cuenta con grupos especializados en seguir la pista a los delincuentes cibernéticos.	1 Aprovechar el crecimiento constante de la tecnología para capacitar de la misma forma a los grupos especializados en seguir la pista a los delincuentes cibernéticos. (F1, O2)		1 Dar a conocer los grupos especializados en seguir la pista a los delincuentes cibernéticos para minimizar la falta de conocimiento o interés de la sociedad (F1, A2)
		ESTRATEGIA DO		**ESTRATEGIA DA**
DEBILIDADES	1 No poseen herramientas para adquirir, preservar y recuperar evidencias digitales. 2 Falta de una política criminal articulada en cuanto al uso de tecnologías. 3 Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático. 4 La entidad no cuenta con procesos y procedimientos que faciliten la indagación y resolución de delitos informáticos.	1 Disminuir la falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático junto con el crecimiento constante de la tecnología. (D3, O2) 2 Diseñar un esquema con procesos y procedimientos que faciliten la indagación y resolución de delitos informáticos a la par con el crecimiento de la tecnología. (D4, O2) 3 Elaboración de una política criminal articulada en cuanto al uso de tecnologías valiendose de la autonomía de la administración de justicia frente al resto de administraciones públicas. (D2, O1)		1 Diseñando un esquema con procesos y procedimientos que faciliten la indagación y resolución de delitos informáticos disminuiría la falta de conocimiento o interés de la sociedad. (D4, A2) 2 Adquirir las herramientas para obtener, preservar y recuperar evidencias digitales ya que son datos intangibles y transitorios. (D1, A3)

ANEXO C - MARCO LÓGICO DEL PROYECTO

Este anexo muestra el Marco lógico del Proyecto, detalla el Fin y Propósito del proyecto. Se establece en el Capitulo 1 – página 42

Marco Lógico del Proyecto				
	Objetivos	**Indicadores**	**Medios de Verificación**	**Supuestos**
Fin				
	Establecer todas las formas de delito informático con herramientas tecnológicas mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los delitos informáticos.	Reducción de un 25% de los juicios sin resolver de delitos informáticos.	Estadísticas de la Corte de Justicia Provincial y Corte Nacional de Justicia.	Las Cortes de Justicia cuentan con un diseño de procedimientos y funciones para indagar los delitos informáticos. Para disminuir los procesos judiciales sobre estos.

Propósito				
	Mejorar la productividad tecnológica y brindar un respaldo al Sistema Judicial del País.	Incremento de un 25% en la utilización de los servicios tecnológicos.	Estadísticas de las empresas que ofrecen servicios informáticos: Cantidad de personas que utilizan estos servicios.	La utilización del diseño de procedimientos y función cumple a cabalidad con indagar los delitos informáticos con la finalidad de cumplir con el 100% en la cantidad de delitos informáticos resueltos con rapidez y eficacia.
Componentes				
1	Identificado y comprendido los problemas de la Administración de Justicia actuales.	100% el informe de evaluación de la situación actual de la Administración de Justicia.	El informe impreso del análisis de la situación actual.	El personal de las instituciones encargadas de la administración de justicia. Colabora en proporcionar información de los procesos

				administrativos, conocimientos y funciones del personal.
2	Procesamiento y selección de la mejor alternativa, según estudio de la situación actual.	100% el informe de análisis de la mejor alternativa.	El informe impreso del análisis de la mejor alternativa.	La alternativa de elaboración del diseño es la más óptima de acuerdo a su nivel de tiempo de ejecución.
3	Creación del diseño del nuevo esquema para el procedimiento de indagación de los delitos informáticos.	100% el diseño terminado.	Manuales completos de las funciones y los procedimientos.	Aprobado el proyecto por directivos de la universidad.
Actividades		**Medios**	**Costos**	
1.1	Comprender bien el problema de la administración de justicia actual.	Recurso Humano	$1.196,00	

1.2	Buscar información actual de los procedimientos y funciones en el caso que hubiere.	Recurso Humano		
1.3	Elaborar la Matriz de Involucrados.	Recurso Humano		
1.4	Elaborar el árbol de problemas.	Recurso Humano		
1.5	Elaborar el árbol de objetivos.	Recurso Humano		
1.6	Procesar la información recopilada.	Recurso Humano		
1.7	Analizar la información recopilada.	Recurso Humano		
1.8	Elaborar el informe de la situación actual de la administración de justicia.	Recurso Humano		

1.9	Elaborar el manual de procedimientos para el nuevo diseño.	Recurso Humano	$400,00	
1.10	Elaborar el manual de funciones para el nuevo diseño	Recurso Humano		

CUESTIONARIOS

ANEXO D - Cuestionario de Cuestionario básico de conocimientos de las TICS del personal de las Instituciones de Administración de Justicia.

Este anexo es de los cuestionarios que se realizaron para obtener los datos de campo. Se establece en el Capitulo 2 – pagina 100.

	ESCALA DE VALORES				
PREGUNTAS	**SI**	**EN PARTE**	**NO**	**N/C**	**OBSERVACIONES**
1. ¿Usted tiene conocimiento de computación?					
2. ¿Maneja usted un computador personal?					
3. ¿Conoce sobre la herramienta de internet?					
4. ¿Maneja internet?					
5. ¿Conoce sobre los delitos informáticos?					
6. ¿Sabe cual son los principales delitos informáticos?					
7. ¿Conoce el marco legal que los regula?					
8. ¿Conoce el delito informático más común?					
9. ¿Sabe dónde las personas encargadas de estos delitos se capacitan?					
10. ¿Ha recibido capacitación sobre los delitos informáticos?					
11. ¿Conoce usted qué es la seguridad informática?					

12. ¿Toma acciones para evitar delitos informáticos?					
13. ¿Conoce alguna actividad cotidiana en el computador que se considere delito?					
14. ¿Conoce usted cómo se procede en un delito informático?					
15. ¿Sabe usted como resguardar evidencias digitales?					
16. ¿Conoce usted qué es una Firma Electrónica?					
17. ¿Ha realizado una transacción electrónica?					
18. ¿Ha tomado precauciones al realizar transacciones digitales?					
19. ¿Conoce la Factura Electrónica?					
20. ¿Tiene usted Correo Electrónico?					

ANEXO E - Cuestionario de conocimientos jurídicos sobre el marco Legal (Leyes) del personal de las Instituciones de Administración de Justicia.

Este anexo es de los cuestionarios que se realizaron para obtener los datos de campo. Se establece en el Capitulo 3 – pagina 100.

	ESCALA DE VALORES				
PREGUNTAS - Conoce usted sobre :	**SI**	**EN PARTE**	**NO**	**N/C**	**OBSERVACIONES**
Delitos contra elementos físicos (Hardware): robo, hurto, estafa, apropiación indebida y daños.					
Delitos contra elementos					

lógicos (Software).					
Daños en sistemas o elementos informáticos, (Art 6 Ley de Comercio Electrónico) en datos, programas o documentos electrónicos (sabotaje informático).					
Acceso ilícito a sistemas informáticos (secretos, derecho a la intimidad, protección de datos, propiedad intelectual e industrial).					
Acceso no autorizado a sistemas informáticos ajenos, utilizando las redes públicas de telefonía o transmisión de datos, burlando las medidas de seguridad, como contraseñas o claves de acceso.					
Las finalidades del hacking.					
Accesos ilícitos a datos que pueden considerarse secretos de empresa.					
Datos que se califican de secretos.					
Procedimientos de fabricación o de investigación de nuevos					

productos.					
Lista de clientes, tarifas, descuentos, distribuidores, estrategias comerciales, modelo de negocio, modo de trabajo, proyectos de expansión.					
Organización interna de la empresa.					
Descubrimiento y revelación de secretos.					
Descubrimiento y revelación de secretos relativos a la defensa nacional.					
Apoderamiento de ficheros con información de valor económico no calificable de secreto de empresa (No Tipificado).					
Estudios generales de mercado, un listado para envés postales, etc.					
Apropiación indebida de uso.					
Protección penal a los programas de ordenador y sus contenidos (piratería).					
Reproducción.					
Plagio.					
Transformación.					

Distribución.					
Comunicación pública.					
Almacén de ejemplares.					
Utilización ilegítima de terminales de comunicaciones (defraudaciones de telecomunicaciones) (No Tipificado).					

ANEXO F - Cuestionario de conocimientos técnicos sobre Informática, Telecomunicaciones y Comercio Electrónico del personal de las Instituciones de Administración de Justicia.

Este anexo es de los cuestionarios que se realizaron para obtener los datos de campo. Se establece en el Capitulo 3 – pagina 100.

	ESCALA DE VALORES				
PREGUNTAS - Conoce usted sobre :	**SI**	**EN PARTE**	**NO**	**N/C**	**OBSERVACIONES**
DELITOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS					
Estafa perpetrada a través de medios informáticos.					
Apoderamiento de Dinero utilizando tarjetas de cajeros automáticos.					
Utilización del correo electrónico con finalidad criminal (No Tipificado).					
Amenazas.					
Injurias.					
Inducción al delito.					

Actos preparatorios y de cooperación para el delito.					
Actividades de extorsión.					
Utilización de Internet como medio criminal (No Tipificado).					
Difusión de contenidos o material ilícito.					
Material pornográfico: difusión, posesión.					
Incitación al odio o a la discriminación.					
Piratería (Instrumento Físico).					
Internet (Instrumento Virtual).					
Robo de Identidad – Phishing.					
Spam.					
Virus.					
Uso comercial no ético – Cybertorts.					
Utilización de Equipos de Telecomunicaciones como medio criminal (No Tipificado).					
Redes.					
TV x IP.					
Voz x IP (Telefonía IP).					
Internet.					
Telefonía Celular.					
Smartphone (Blackberrys y teléfonos inteligentes, PDA).					

Servicios inalámbricos (Bluetooth, WIFI, WIMAX).					

ANEXO G - DIRECCIÓN DE LA ENCUESTA AL PÚBLICO EN GENERAL

Este anexo es de los cuestionarios que se realizaron para obtener los datos vía web. Se utilizo la herramienta **Google Docs.** Se establece en el Capitulo 3 – pagina 101.

Enlace: https://docs.google.com/spreadsheet/viewform?formkey=dGplTHVYS2N3T0ptS1lGR3FYU0tjeUE6MQ

ENCUESTA SOBRE SEGURIDAD INFORMÁTICA

* Required

Tiempo de trabajo:

Tipo de trabajo:

Edad:

Estudios:

¿Usted tiene conocimiento de computación? *

- Si
- En parte
- No
- No contesta

¿Conoce sobre la herramienta de internet?

- Si
- En parte
- No
- No contesta

¿Maneja internet?

- Si
- En parte
- No
- No contesta

¿Sabe usted que es un delito informático?

- Si
- En parte
- No
- No contesta

¿Sabe cual son los principales delitos informáticos?

- Si
- En parte
- No
- No contesta

¿Ha sido víctima de algún delito informático?

- Si
- En parte
- No

- No contesta

¿Sabe dónde dirigirse en el caso de ser víctima de algún delito informático?

- Si
- En parte
- No
- No contesta

¿Conoce usted qué es la seguridad informática?

- Si
- En parte
- No
- No contesta

¿Toma acciones para evitar delitos informáticos?

- Si
- En parte
- No
- No contesta

¿Ha realizado una transacción electrónica?

- Si
- En parte
- No
- No contesta

¿Siente seguridad al realizar transacciones electrónicas?

- Si

- En parte
- No
- No contesta

¿Ha tomado precauciones al realizar transacciones electrónicas?

- Si
- En parte
- No
- No contesta

¿Tiene usted correo electrónico?

- Si
- En parte
- No
- No contesta

¿Utiliza con frecuencia su correo electrónico?

- Si
- En parte
- No
- No contesta

¿Alguna vez ha sido bloqueado su correo electrónico?

- Si
- En parte
- No
- No contesta

¿Pese a los problemas actuales sobre los delitos informáticos utilizaría o seguiría utilizando servicios vía web?

- Si
- En parte
- No
- No contesta

ANEXO H - DATOS ENTREVISTADO

Este anexo es los datos del Entrevistado, conocedor de los delitos informáticos. Se establece en el Capitulo 3 – pagina 217.

Roberto Olaya

CEO en HCKS Seguridad Lógica

Ecuador

Seguridad del ordenador y de las redes

VOCABULARIO

Adiestramiento.- Enseñanza o entrenamiento de una habilidad manual o un ejercicio físico.

Antijurídica.- Contrario al Derecho.

Atañen.- Tocar a una persona una responsabilidad u obligación, o una cosa que tiene interés para ella.

Criminalística.- Se definen como los conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes cometen los delitos.

Criminología.- Trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito.

Criptología.- Sistema que ofrecen medios seguros para la comunicación en los que el emisor oculta o cifra un mensaje antes de transmitirlo para que un receptor autorizado o nadie puedan verlo.

Déficit.- Situación en la que falta o hay escasez de una cosa necesaria.

Delinquir.- Cometer una acción que va contra la ley.

Disertación.- Razonamiento que se hace sobre una materia de forma detenida y siguiendo un orden o un sistema para exponerlo.

Desvirtuación.- Disminuir o quitar la virtud o las características esenciales de una cosa.

Empíricos.- Que es un resultado inmediato de la experiencia, que solo se funda en la observación de los hechos.

Ente.- Organismo, institución o empresa, generalmente de carácter público.

Estatuto jurídico.- Son normas sobre las que se rigen las instituciones jurídicas, pueden ser diferentes para cada institución; normas internas.

Esteganografía.- La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Experticia.- Prueba pericial.

Extorción.- Presión que se hace a una persona, mediante el uso de la fuerza o la intimidación, para conseguir de ella dinero u otra cosa.

Extradición.- Entrega de una persona refugiada o detenida en un país a las autoridades de otro que la reclama para juzgarla.

IDE.- Son discos duros cuya electrónica de manejo está incorporada al propio disco, por lo que son los más económicos.

Inversor.- Que invierte. Cambiar, sustituyéndolos por sus contrarios, la posición, el orden o el sentido de las cosas.

Indagación.- Conjunto de preguntas e investigaciones que se llevan a cabo para conocer datos o informaciones; especialmente si son referentes a un asunto oculto o secreto.

Ingentes.- Que es muy grande o numeroso.

Ilícitas.- Que no está permitido por la ley o la moral.

Jurídica.- Que atañe al derecho o se ajusta a él.

Jurídico.- Relacionado con las leyes y el Derecho.

Jurisdicción.-Territorio en el que se ejerce una autoridad para gobernar y hacer ejecutar las leyes.

Jurisdiccional.- Relativo a la jurisdicción.

Meridiana.- Hacer que una cosa difiera en algo de lo que antes era.

Misceláneos.- Mixto, vario, compuesto de cosas distintas o de géneros diferentes.

Legislación.- Conjunto de las leyes de un Estado y también conjunto de leyes relativo a una materia determinada. Estos conjuntos comprenden no solo las leyes propiamente dichas, sino también las normas consuetudinarias y las normas de carácter ejecutivo (reglamentos, etc.).

Paradigma.- Ejemplo que sirve de norma o modelo.

Pericia.- Sabiduría, práctica, experiencia y habilidad en una ciencia o arte.

Pericial.- Relativo a perito. Ciencia o arte.

Perito.- Se aplica a la persona que tiene experiencia, práctica o habilidad en determinada.

Peritaje.- Trabajo o estudio que hace un perito.

Posix.-Sistema operativo multitarea y multiusuario. Adecuado para ser empleado en micro y miniordenadores.

Postre.- A lo último, al fin.

Relegada.- Apartar o dejar de lado a una persona o una cosa.

SCSI.- Son discos duros de gran capacidad de almacenamiento (desde 5 Gbyte hasta 23 Gbytes).

Skimmers.- pequeño dispositivo electrónico PARA obtener un número de tarjeta de crédito.

Suplantación.- Acción que consiste en hacerse pasar una persona por otra para obtener algún beneficio.

Tipificación.- Conjunto de características que son representativas de un modelo o clase.

Transitorios.- Que dura relativamente poco tiempo.

Transgresores.- Que quiebra o actúa en contra de una ley, norma o regla.

Vestigios.- Señal o resto que queda de una cosa pasada o antigua.

Volátiles.- Se aplica al carácter u opinión que cambia mucho o es inconstante.

ZIP.- Formato de compresión ZIP, un método muy utilizado para comprimir archivos informáticos.