UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA:

INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

“EL ROL DE LA AUDITORÍA FORENSE ANTE LOS NUEVOS DELITOS INFORMÁTICOS TIPIFICADOS EN EL ACTUAL CÓDIGO ORGÁNICO INTEGRAL PENAL DEL ECUADOR COIP, METODOLOGÍAS Y HERRAMIENTAS A USAR ANTE UNA EVIDENCIA DIGITAL”

AUTORES:

JAIME JONATHAN ESPINOZA VILLAMAR
RÓMULO GABRIEL VERDEZOTO ACUÑA

DIRECTOR:

ING. MOISES TOAPANTA, MSc.

Guayaquil, Abril de 2015

DECLARATORIA DE RESPONSABILIDAD

Nosotros autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaramos que los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo, son de exclusiva responsabilidad de los autores.

Guayaquil, Abril de 2015

_____	_____
Jaime Espinoza Villamar	Rómulo Verdezoto Acuña

AGRADECIMIENTO

Quiero agradecer primero a Dios que fue el que me guió durante todo este camino lleno de batallas y continuas luchas ante adversidades que se presentaron en esta etapa de estudio.

A la Universidad Politécnica Salesiana, Facultad de ingenierías, por habernos abierto las puertas y así poder concluir nuestros estudios profesionales.

A mis instructores, docentes y demás educadores en especial a la MSc. Laura Ureta por su valiosa ayuda en la elaboración de esta tesis, de igual forma al Ing. Joe Llerena por su motivación constante durante mis estudios universitarios.

A mi Tutor, Ing. Moisés Toapanta, MSc. Quien nos brindó su apoyo para poder realizar de la mejor manera el proyecto de tesis.

Jaime Espinoza V.

AGRADECIMIENTO

Agradezco infinitamente a Dios, el principal guía en el camino hacia la consecución de mis objetivos, por ser quien me dio la salud, la vida y el intelecto para alcanzarlos. Porque siempre estuvo y está allí cuando más lo necesito y en cada paso que doy.

A nuestro tutor, por direccionarnos y ofrecernos las pautas de nuestro tema de investigación.

A todos mis familiares, amigos, y en especial a mi compañero de tesis, Jaime Espinoza, a todos por creer en mí y por ofrecerme ese granito de arena que me impulsa cada día a salir adelante.

Rómulo Verdezoto A.

DEDICATORIA

Dedico este proyecto de tesis a Dios y a mi Familia que siempre han estado conmigo apoyándome incondicionalmente.

A mis padres, Jaime Espinoza y Cristina Villamar, que siempre me apoyaron y alentaron para alcanzar esta meta, ambos son mis motivos para seguir adelante.

A toda mi familia, ya que siempre me impulsaron el estudio y me sirvieron de guía para ser un hombre de bien.

Jaime Espinoza V.

DEDICATORIA

Dedico este trabajo, con el más sincero agradecimiento, a Dios. Sé que sin Él, nada en mi vida hubiese sido posible.

A toda mi familia, que han depositado toda su confianza en mí ya que jamás dudaron o dudarán que proponiéndomelo, puedo lograr cualquier objetivo que tenga en la vida y que saben que cada día puedo dar más de mí.

En especial, deseo dedicar este trabajo a mis padres, quienes han sido parte fundamental en mi vida al estar siempre conmigo dándome su apoyo y consejo, pero sobre todo, siendo el más grande ejemplo de que cuando se hacen las cosas con amor y en presencia de Dios, todo en la vida tiene sentido.

Rómulo Verdezoto A.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE FIGURAS

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto de tesis tiene como objetivo estudiar, analizar y exponer en qué consiste la Informática Forense, los conceptos que la definen, y cómo a través de ella se encuentran evidencias ante un delito informático, especialmente sobre los últimos tipificados en el actual Código Orgánico Integral Penal del Ecuador, su metodología y las herramientas que permiten llevar a cabo una investigación forense digital, de forma tal que sea posible la identificación de los diversos riesgos que constituyen una amenaza a la validez de la evidencia, la cual deberá ser presentada ante un tribunal de justicia.

Además, se procede a abordar la formación de los peritos o especialistas que investigan dichos delitos, los organismos autorizados para la acreditación de los mismos, así como las repercusiones legales que podrían presentarse en el ejercicio de la profesión como perito informático.

Abordaremos las herramientas más conocidas disponibles en el mercado y que son indispensables para recolectar la evidencia digital, considerando que la recolección de evidencia en el sitio del crimen es una da las tareas más críticas en el proceso de investigación, por lo que dicha evidencia debe ser idéntica a la original y debe permanecer inalterada la escena del crimen, por lo antes dicho, es necesario que el perito forense conozca las herramienta disponibles y cual debe aplicar en cada caso.

Adicionalmente, analizaremos como la legislación debe ir avanzando a la realidad actual del mundo, y a su vez buscar una salida jurídica mediante el acceso a la justicia por medio de los Órganos Jurisdiccionales correspondientes y el respeto a la Ley.

PALABRAS CLAVE:

Auditoría Forense, Evidencia Digital, Perito Informático, Cadena de Custodia, Certificados de Seguridad, Activo electrónico Patrimonial, Delito informático.

ABSTRACT

The goal of this project is to study and analyze by presenting and explaining about Computer Forensics, its definition and how we can find evidence of a cyber-crime through it. It is about the last six established in the current Penal Integral Organic Code specially; its methodology and the tools let to do a computer forensics investigation getting the identification of the different risks that are threats for the validity of the evidence, this should be presented on a justice court.

Besides, it is going to proceed to address the training of the experts or specialists, who investigate these crimes, the authorized organisms for the accreditation of thereof, and the legal repercussions that could arise in the practice of the profession as a computer expert.

The most popular tools available on the market will be reviewed, also necessary for gathering digital evidence, always taking into account that the harvest of evidence at a crime scene is one of the most critical and fundamental tasks in the investigation process, because said evidence must be identical to the original and the crime scene must remain unaltered. It is therefore necessary that the forensic investigator must know the available tools and which ones to utilize in each case.

In addition, we will analyze the Legislation must go advancing to the current reality of the world, and in turn look for a juridical exit by means of the access to the justice by means of the Courts and that this goes of the hand with the Law.

KEYWORDS:

Forensic Audit, Digital Evidence, Computer proficient, Chain of Custody, Security Certificates, Asset-mail Active, Computer crime.

INTRODUCCIÓN

En los actuales tiempos se observa la gran influencia que ha logrado la informática en la vida cotidiana de las personas, asimismo en el contexto de las empresas y entes gubernamentales, de manera que hasta se podría considerar que la informática es una ciencia que aporta de modo directo al desarrollo de un país.

Conforme los avances tecnológicos aumentan, éstos cada vez tienen mayor incidencia en muchas áreas de la vida social, lo que origina diversos tipos de comportamientos, los mismos que pueden clasificarse como actos delictivos y no delictivos, los primeros se han catalogado a nivel general como "delitos informáticos".

Este tipo de comportamientos que evolucionan continuamente a una velocidad imparable, han logrado que distintas ciencias traten no sólo de interpretar el accionar de los ejecutores, sino que adicional, han encaminado el poder construir mecanismos o procedimientos con la finalidad de prevenir los variados tipos de actos ilícitos que son llevados a cabo sobre diferentes dispositivos informáticos.

La informática forense aparece como una disciplina complementaria para la justicia en los actuales momentos, donde los delitos han variado y surgen distintas figuras legales, tal es el caso de nuestro actual Código Orgánico Integral Penal, donde se tipifican 6 nuevos delitos informáticos con el fin de mitigar y castigar el cometimiento de los mismos.

En el capítulo 1 se detallan los elementos primordiales de nuestro estudio, tales como, el planteamiento del problema, el objetivo general y los específicos por lo que planteamos la elaboración de esta guía, así como la justificación de la misma.

En el capítulo 2 se abordará el marco teórico de los delitos informáticos, de la Informática Forense y las leyes relacionadas que se encuentran establecidas en la legislación ecuatoriana.

En el Capítulo 3 nos referiremos a los especialistas o peritos, el perfil solicitado o requerido, las Instituciones de acreditación, los requisitos para poder acreditarse, e igualmente se tratarán las implicaciones legales y las causas por las que al especialista se le podrían retirar sus credenciales.

En el Capítulo 4, abordaremos los nuevos delitos informáticos del actual COIP y la diferenciación entre la naturaleza de los causantes de dichos delitos, asimismo se explican las iniciativas gubernamentales respecto a la conformación del Comando de Ciberdefensa para proteger la seguridad del estado ecuatoriano ante cualquier ataque cibernético.

El proyecto de tesis finaliza con diversas conclusiones, producto de la experiencia en el desarrollo de este proyecto, de igual forma varias recomendaciones basadas en los estudios realizados, comentarios y sugerencias de peritos informáticos y especialistas en derecho informático, con el objetivo de que el lector asimile la relevancia, pertinencia y vigencia de lo expuesto en este proyecto.

CAPÍTULO I

EL PROBLEMA

1.1. Planteamiento del problema

Las personas naturales, empresas y gobiernos hacen uso de un vasto número de sistemas informáticos para la ejecución de sus operaciones o a su vez almacenamiento de datos, y a medida que esta demanda aumenta, hacen que, ya sea sus equipos informáticos, programas y/o aplicaciones, sean vulnerables a ataques e incidentes que pongan en riesgo la integridad de dichos componentes, ocasionando así daños en las plataformas tecnológicas, pérdidas económicas, etc. Por estas razones se le debe otorgar la consideración necesaria para implementar normas de seguridad, establecer planes de respuesta inmediata y asegurar un marco legal apropiado para proteger o salvaguardar las infraestructuras tecnológicas así como la integridad de la información.

Conforme se incrementa y varía el uso de herramientas y recursos tecnológicos, las vulnerabilidades y amenazas aparecen permanentemente. Los hackers o usuarios mal intencionados buscan servicios mal configurados, contraseñas poco robustas, vulnerabilidades en los protocolos de sistemas operativos, utilizando además a su favor, la carencia en la cultura sobre seguridad informática que existe en la sociedad. Citando los incidentes y ataques más comunes que deben considerarse para mantener la seguridad de un equipo o sistema informático, tenemos: troyanos, virus y gusanos, robo de contraseñas, backdoors, ataques de denegación de servicios (DOS), correo no deseado, sniffing, buffer overflow e IP spoofing, entre otros.

Para hacer frente y determinar las causantes de este tipo de ataques, que en nuestro país se consideran como delitos informáticos, existe la Informática Forense como una vía clave en la investigación de estas prácticas ilícitas. Esta ciencia trata acerca de la aplicación de técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos que sean una evidencia digital llevando así a la solución judicial del delito padecido.

1.2. Formulación del Problema

De qué manera la Informática Forense puede contribuir a la obtención de resultados eficientes en los procesos judiciales, considerando la inclusión de nuevos delitos informáticos en el actual Código Orgánico Integral Penal del Ecuador.

De acuerdo a varias estadísticas proporcionadas por la Fiscalía General del Estado y que han sido mostradas en varios medios de comunicación, se llegó a determinar el impacto exponencial que nuestro país ha venido enfrentando respecto a los delitos informáticos y que espera disminuir su cometimiento al incluir nuevos delitos de esta índole en el actual Código Orgánico Integral Penal.

Para determinar el problema se procedió a cuantificar los incidentes más conocidos a nivel nacional desde el período 2011 - 2014 relacionados a nuestro tema de estudio, entre los que tuvieron mayor connotación tenemos:

- Claves de Acceso en Municipio de Riobamba – *16 de abril del 2013.*
- Caso "El Universo" – *6 de febrero del 2011.*
- Alteración del Sistema de calificaciones de la UESS – *7 de marzo del 2013.*
- Allanamiento a domicilio de Fernando Villavicencio (incautación de laptops) – *27 de diciembre del 2013.*
- Hackeo a varios sitios web de instituciones públicas, entre otros. - *Agosto del 2012.*

1.3. Objetivos

1.3.1 Objetivo general

Elaborar una guía de estudio para analizar y exponer en qué consiste la informática forense y el rol que ésta desempeña ante los nuevos delitos informáticos descritos en el actual Código Orgánico Integral Penal del Ecuador COIP.

1.3.2 Objetivos específicos

- Detallar y describir las mejores prácticas que permiten efectuar una investigación forense digital de modo que se permita identificar los diferentes riesgos que conformen una amenaza a la integridad y autenticidad de la evidencia, la que deberá ser expuesta ante un tribunal de justicia.
- Mostrar de forma global el estado actual de los delitos informáticos en el Ecuador en cuanto a su regulación, iniciativas de investigación, tecnología y la formación de los especialistas que investigan dichos delitos.
- Determinar los desafíos que el Ecuador deberá superar para el procesamiento de los delitos informáticos, a pesar de las nuevas tipificaciones del COIP.
- Demostrar mediante un caso práctico diferentes herramientas frecuentemente utilizadas para el análisis de una evidencia digital; Imagen bit a bit de un allanamiento.

1.4. Justificación

La aplicación de la informática forense es un tema parcialmente nuevo en el Ecuador, por lo que esta tesis pretende convertirse en una guía para investigaciones o análisis posteriores.

El presente análisis se justifica debido al uso de recursos informáticos por parte de personas en general, organizaciones e instituciones gubernamentales, los cuales requieren ser estructurados a través de medidas y políticas de seguridad, para así proteger y salvaguardar su continua operatividad.

Dar a conocer a la Informática Forense como una valiosa herramienta con el fin de obtener óptimos resultados en el esclarecimiento de un delito informático.

Se justifica debido a que varios de los nuevos delitos informáticos se encuentran tipificados en el reciente Código Orgánico Integral Penal del Ecuador, existen varios tópicos que se prestan a ambigüedades, lo cual genera una brecha en el accionar de las instituciones judiciales.

La utilización de herramientas para la informática forense es una de las metas trazadas para la realización de esta tesis, y mediante la demostración de un caso práctico pretendemos mostrar las bondades y alcances de las herramientas mayormente usadas por parte de los peritos informáticos.

CAPÍTULO II

MARCO TEÓRICO

2.1 Delitos Informáticos

El salto exponencial que la sociedad ha experimentado en un contexto tecnológico, supone un avance en las formas de violar la ley, dando cabida así, tanto a la variación de los delitos comunes, como a la llegada de nuevos actos ilícitos. Esta situación ha originado una discusión en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su manejo dentro de un marco jurídico.

Distintos autores e instituciones han conceptualizado los delitos informáticos, contribuyendo distintas perspectivas a su definición. Algunos contemplan que es trivial distinguir los delitos informáticos de los habituales, por lo que, según estos autores se tratan de los mismos delitos, ejecutados a través de otros medios.

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". El mismo que define los delitos informáticos como:

> *Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de los mismos.* (Convenio de Ciberdelincuencia del Consejo de Europa, 2007)

Otra definición avalada por Instituciones como el B.I.D. es la que hace la Dra. Ma. De la Luz Lima, la cual se denota en el párrafo siguiente:

> *El 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"* (Lima, 1994)

Cabe destacar que no existe un concepto universal de delito informático, aunque, es preciso enfatizar que han sido los empeños de varios especialistas que han abordado el tema y han descrito definiciones prácticas, atendiendo contextos nacionales específicos; asimismo, es valioso revelar que la última definición por parte del Convenio de Ciberdelincuencia del Consejo de Europa hace hincapié en la confidencialidad, integridad y disponibilidad, los cuales son los pilares de la seguridad de la información.

Los delitos informáticos implican acciones de tipo criminal por lo que varios países han tratado de ubicarlos en figuras típicas, tales como: falsificaciones, fraudes, hurto, suplantación, estafa, robos, entre otros; por lo tanto, es imprescindible destacar que el mal uso de las computadoras es lo que ha obligado la necesidad de fijar regulaciones en un marco legal.

De igual manera, es relevante indicar que se han propuesto distintas expresiones para mencionar las conductas ilegales en las que se usa un equipo informático, las más habituales son: "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el ordenador", entre otras.

El Artículo Científico "An Ontology of Information Security" el cual es referenciado por la JCR (Journal Citation Reports) a través de la revista indexada "International Journal of Information Security", aborda lo mencionado en los párrafos precedentes, considerando que la ontología informática hace referencia a la formulación de un riguroso esquema conceptual dentro de uno o varios dominios, con el fin de facilitar la comunicación entre diferentes entidades. Es así que en el artículo se menciona lo siguiente: "En el ámbito de la seguridad de la información muchos conceptos son raramente definidos, incluso por los mismos especialistas".

2.1.1 Tipos de Delitos Informáticos

El Convenio de Ciberdelincuencia del Consejo de Europa 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
- Delitos relacionados con el contenido
- Delitos relacionados con la falsificación y fraude
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

María de la Luz Lima, presenta una clasificación, de los que ella llama "delitos electrónicos" mencionando que existen tres categorías, a saber:

- Los que utilizan la tecnología electrónica como método (Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito).
- Los que utilizan la tecnología electrónica como medio (Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo) y,
- Los que utilizan la tecnología electrónica como fin (conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica).

Diversos especialistas y organismos (Naciones Unidas, Convenio del Consejo de Europa, entre otros.) han clasificado de diferentes maneras los tipos de delitos informáticos conforme variados principios, concordando entre los más significativos los siguientes:

Tabla 2.1. Tipificación de delitos Informáticos

Reconocidos por las Naciones Unidas - Abogados especializados en delitos informáticos	
Fraudes mediante la manipulación de computadores (programas, datos de entrada y salida, repetición automática de procesos).	Fraudes mediante la manipulación de computadoras: 1. Delitos contra elementos físicos – Hardware (robo, estafa) 2. Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos, protección de programas).
Falsificaciones informáticas (alteración de documentos, falsificación de documentos).	

Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)	Delitos cometidos a través de sistemas informáticos: 1. Estafas 2. Apoderamiento de dinero por tarjetas de cajero 3. Uso de correo electrónico con finalidad criminal 4. Utilización de internet como medio criminal
Accesos no autorizados a servicios y sistemas informáticos (piratas, reproducción no autorizada).	

Fuente: Organización de Naciones Unidas

Considerando como referencia la tipificación de los delitos informáticos, los mismos se clasifican de la siguiente manera:

- Fraudes:- Delitos de estafa a través de la maniobra de datos o programas para la obtención de un lucro ilícito (caballos de troya, falsificaciones, etc.).
- Sabotaje informático:- Daños mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc.).
- Espionaje informático:- Divulgación no autorizada de datos reservados.
- Pornografía Infantil:- Inducción, promoción, producción, venta, distribución, facilitamiento de prostitución, cuando se utilizan menores con fines de exhibicionistas o pornográficos.
- Infracciones de Propiedad Intelectual:- Copia o reproducción no autorizada de programas informáticos de protección legal.

2.1.2 Investigación tecnológica de los delitos informáticos

Los componentes de prueba en un proceso son de significativa relevancia, por lo que mediante su investigación se puede dilucidar la comprobación de lo que corresponde a la veracidad de lo ocurrido. Es esencial, considerar la formalidad de las técnicas o procedimientos de análisis utilizados en un proceso de investigación, para así ofrecer mayor claridad y exactitud a las observaciones dentro del proceso, ante el cometimiento de un delito informático.

Estar al tanto de cómo los incidentes de seguridad y la criminalidad informática evolucionan es preciso para el análisis de los delitos informáticos, por lo que en los últimos años han resurgido con mayor fuerza, debido a aquello se requiere estudiar la tendencia de estos componentes.

El Informe Anual de Seguridad de Cisco2015, presenta las investigaciones, perspectivas y sugerencias proporcionadas por expertos acerca de los delitos informáticos, analiza la rivalidad entre atacantes y defensores, y cómo los usuarios son cada vez el eslabón más débil de la cadena de seguridad. En este estudio uno de los factores abordados son los correos electrónicos con fines publicitarios o comerciales enviados a un gran número de destinatarios o también denominados spam, en el informe se indica que "Los volúmenes de spam en todo el mundo están en aumento, lo que indica que el spam sigue siendo un factor lucrativo para los delincuentes en línea, los atacantes siguen generando mensajes para que el spam sea más propenso a engañar a los destinatarios y así logren ejecutar links peligrosos, a menudo haciendo uso de ingeniería social".

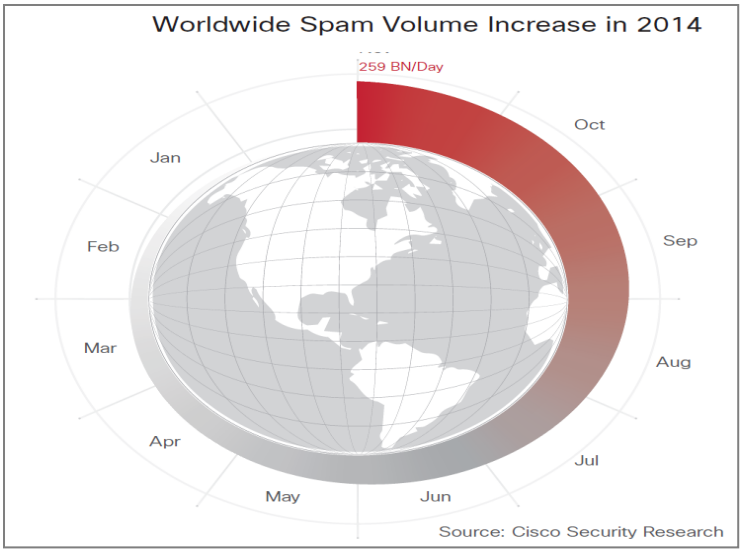
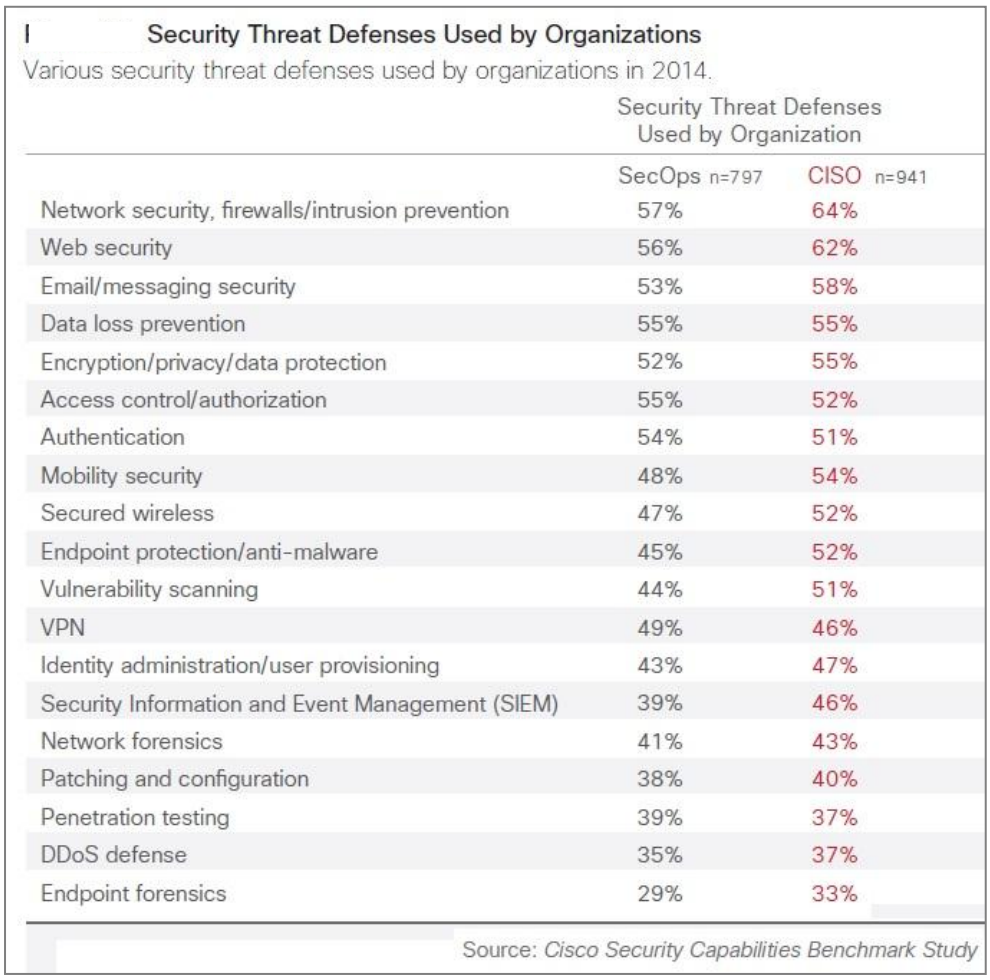


Figura 2.1: Aumento del Volumen de Spam en todo el mundo en el 2014

Fuente: Informe Anual de Seguridad de Cisco 2015

Cisco, en su estudio anual también recoge los mecanismos que las Instituciones están utilizando para no ser víctimas de delitos informáticos y con esto mitigar los niveles de ocurrencia; en la siguiente imagen se ilustra lo antes mencionado:



Security Threat Defenses Used by Organizations

Various security threat defenses used by organizations in 2014.

	Security Threat Defenses Used by Organization	
	SecOps n=797	CISO n=941
Network security, firewalls/intrusion prevention	57%	64%
Web security	56%	62%
Email/messaging security	53%	58%
Data loss prevention	55%	55%
Encryption/privacy/data protection	52%	55%
Access control/authorization	55%	52%
Authentication	54%	51%
Mobility security	48%	54%
Secured wireless	47%	52%
Endpoint protection/anti-malware	45%	52%
Vulnerability scanning	44%	51%
VPN	49%	46%
Identity administration/user provisioning	43%	47%
Security Information and Event Management (SIEM)	39%	46%
Network forensics	41%	43%
Patching and configuration	38%	40%
Penetration testing	39%	37%
DDoS defense	35%	37%
Endpoint forensics	29%	33%

Source: *Cisco Security Capabilities Benchmark Study*

Figura 2.2: Defensas ante amenazas de seguridad usadas por Organizaciones

Fuente: Informe Anual de Seguridad de Cisco2015

2.1.2.1 La Evidencia Digital

Al igual que para los delitos informáticos se han establecido diferentes definiciones, asimismo se han producido varias connotaciones para su principal factor: la evidencia digital.

El especialista forense y autor del Libro "Digital Evidence and Computer Crime" Eoghan Casey, define en su libro a la evidencia digital como:

> *"Un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales."*(Casey, 2004)

A más de lo mencionado por Casey, se debe tener en cuenta que la misma sirve en los procesos judiciales con el fin de demostrar un hecho en particular y que debe ser obtenida mediante la aplicación de rigurosos y metodológicos procesos que aseguren su validez.

De igual forma, en el libro Introducción a la Informática Forense, del autor Jeimy Cano, Phd. Se indica lo siguiente:

> *La evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable.* (Cano J. , 2006)

Estas propiedades indican la exigente labor que se requiere por parte de los especialistas en materia de informática forense, ya sea en procedimientos, como en técnicas y herramientas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. De igual forma, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado a: su debido registro, admisibilidad, valor probatorio, preservación, transformación y recuperación.

2.1.2.2 La informática Forense

Uno de los organismos especializados en el tema de la Informática Forense es el F.B.I. (*Federal Bureau of Investigation*), organismo que incluso ha desarrollado soluciones informáticas que permiten examinar evidencia computacional, este ente define a la Informática Forense como se detalla a continuación:

> *"Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio informático"*(F.B.I., 1997)

Parcialmente nueva, esta ciencia se aplica ya sea en las investigaciones de delitos comunes como: narcotráfico, fraudes financieros, extorsión, etc.; así como para

aquellos que están inherentemente relacionados con las TIC's, de las más conocidas: tráfico de bases de datos, piratería de software, distribución de pornografía infantil, entre otras.

Por lo tanto, el cumplimiento de la informática forense, se denomina como una técnica la cual es usada por los peritos mientras se lleva a cabo el proceso de investigación de los delitos informáticos.

Para el autor de varias publicaciones y especialista en la rama forense, el español Miguel López Delgado, el análisis forense digital es:

> *"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"*(López, 2007)

Las etapas relativamente importantes que se definen en un proceso de análisis forense son las que se describen en la siguiente imagen:

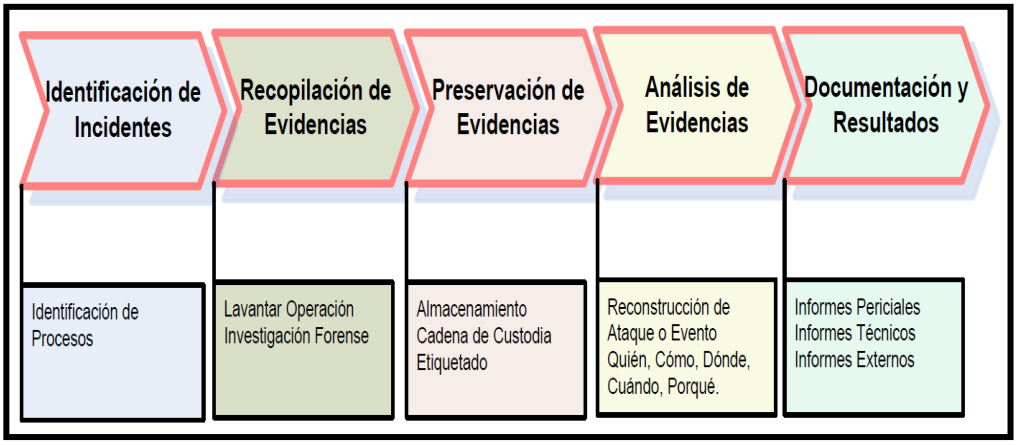


Figura 2.3: Fases del Análisis Forense Digital

Fuente: (López, Análisis Forense Digital, 2007)

2.1.2.2.1 Identificación de Incidentes

En la etapa inicial se deberá confirmar la integridad de la evidencia original, por lo tanto, no sería acertado efectuar modificaciones, cambios o transformaciones en dicha evidencia, sino más bien conservar los requerimientos jurídicos.

Asimismo, es imprescindible que el especialista o perito se cuestione acerca de la información recogida dentro de un sistema implicado.

Se deberán identificar los procesos que se encuentran "corriendo" en el dispositivo ante un incidente y lograr reconocer alguna instrucción o tarea ajena o poco usual, por lo tanto es imperioso estar al tanto de la actividad propia del sistema. Así tenemos que, dentro de las primordiales tareas de esta etapa, se deberá analizar los registros del sistema, accesos no permitidos, conexiones no exitosas, modificaciones a archivos propios del sistema, etc.

2.1.2.2.2 Recopilación de Evidencias Digitales

En el caso que se confirme que el sistema esté comprometido, en base a las pruebas realizadas en la fase inicial (identificación de incidencias), se deberá identificar la prioridad entre las alternativas de: levantar la operación del sistema o efectuar una investigación forense al detalle.

- Por lo general, la primera acción a realizar es restablecer el sistema a su curso habitual, sin embargo, se debe tener presente que aquello pueda ocasionar que se pierdan casi todas las evidencias que todavía se encuentren en la "escena del delito" e inclusive puede ocasionar la limitante de efectuar las acciones jurídicas correspondientes.

- De suscitarse la elección por la segunda opción y el perito es apto para ejecutarlo, se deberá empezar con la recopilación de las evidencias que puedan precisar los métodos de entrada, acciones realizadas por el o los intrusos, duración del incidente o suceso, pero ante todo tomando las precauciones para evitar modificar las evidencias en el transcurso de la fase de recopilación.

Se debe asegurar el llevar un registro de todas las acciones realizadas, así como de los datos o información encontrada, es necesario procurar la obtención del mayor número de datos o información posible, de esta forma también es aconsejable que

mientras se realiza el desarrollo de este procedimiento, lo secunde una persona, neutral e imparcial, que cumpliría las funciones de testigo de los actos y procesos ejecutados.

Al llevar a cabo esta etapa, es aconsejable emplear una metodología de recopilación de evidencias, para esto, el especialista debe hacer uso de habilidades o métodos que sean reconocidas y que puedan ser replicadas en el mismo entorno del escenario presente.

Para la recolección de evidencias se cuenta con marcos de trabajo de libre distribución, los cuales han sido desarrollados considerando las mejores prácticas. La siguiente tabla registra algunos de los marcos con reconocimiento a nivel mundial para la recolección de evidencias en computación forense:

Tabla 2.2. Guía de mejores Prácticas de Computación Forense

GUÍA	PATROCINADOR	DISTRIBUCIÓN
RFC 3227 – Guía para recolectar y archivar evidencia	Network Working Group http://www.ietf.org	Libre
Guía IOCE – Guía de mejores prácticas en el examen forense de tecnología digital	International Organization on Computer Evidence http://www.ioce.org	Libre
Guía DoD1 – Investigación en la escena del crimen electrónico	U.S. DoJ http://www.usdoj.gov	Libre
Guía DoJ2 - Examen forense de evidencia digital	U.S. Department of Justice http://www.usdoj.gov	Libre
Guía Hong Kong Computación Forense – Parte 2 – Mejores Prácticas	SWGDE – Scientific Working Group on Digital Evidence http://www.acpo.police.uk	Libre
Guía Reino Unido – Guía de buenas prácticas para evidencia basada en computadoras	ACPO – Association of Chief Police Officers http://www.acpo.police.uk	Libre
Guía Australiana – Guía para el manejo de evidencia en IT	Estándar Australiano http://unpan1.un.org	Pago
Norma ISO/IEC 27037:2012	ISO/IEC http://www.iso.org	Pago

Fuente: (Watson D. , Digital Forensics Processing and Procedures, 2013)

A continuación se detallan las guías más reconocidas en relación al cómputo forense a nivel mundial:

2.1.2.2.2.1 RFC 3227

El RFC 3227 es una Guía para recolectar y archivar evidencia, fue elaborado en el 2002 por los ingenieros del Network Working Group. Dentro de la guía recogemos las siguientes acciones recomendadas:

- No apague el sistema hasta que la recolección de la evidencia se haya completado.
- Ejecute programas de recolección de evidencias apropiados
- No ejecute programas que modifiquen las fechas de acceso a todos los archivos del sistema.

En este marco, se hace énfasis en la transparencia que debe existir en esta etapa, debido a que los métodos usados para recopilar o reunir pruebas deben ser transparentes y reproducibles; se debe estar preparado para reproducir con exactitud los métodos que se utilizaron, y poder lograr que esos mismos métodos puedan ser efectuados por expertos independientes.

En cuanto a la Cadena de Custodia, la guía especifica que se debe ser capaz de describir claramente cómo se encontró la evidencia, la forma en que se manejó y todo lo ocurrido con la evidencia, de igual forma se especifica la necesidad de ser documentado lo siguiente:

- ¿Dónde, cuándo y por quién fue la evidencia descubierta y se recoge?
- ¿Dónde, cuándo y por quién fue la evidencia manejada o examinada?
- ¿Quién tenía la custodia de la evidencia, durante qué período, cómo se almacena?
- Cuando la evidencia cambia la custodia, cuándo y cómo se produjo la transferencia.

2.1.2.2.2.2 Guía IOCE

La *International Organization of Computer Evidence* -IOCE- por sus siglas en inglés, promulgó la "Guía para las mejores prácticas en el examen forense de tecnología digital" (*Guidelines for the best practices in the forensic examination of digital technology*)", la guía proporciona una serie de estándares, principios de calidad y aproximaciones para la detección, prevención, recuperación, examinación y uso de la evidencia digital para fines forenses.

Cubre los sistemas, procedimientos, personal, equipo y requerimientos que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte. Su estructura es:

- Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
- Determinación de los requisitos de examen del caso.
- Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
- Prácticas aplicables al examen de la evidencia de digital.
- Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
- Priorización de la evidencia.
- Examinar la evidencia: protocolos de análisis y expedientes de caso.
- Evaluación e interpretación de la evidencia
- Presentación de resultados (informe escrito).
- Revisión del archivo del caso: Revisión técnica y revisión administrativa.
- Presentación oral de la evidencia.
- Procedimientos de seguridad y quejas.

De toda esta estructura se puede rescatar en general 4 fases principales:

- Recolección de la evidencia sin alterarla o dañarla.
- Autenticación de la evidencia recolectada para asegurar que es idéntica a la original.
- Análisis de los datos sin modificarlos.
- Reporte final.

2.1.2.2.2.3 Guía DoJ 1

El Departamento de Justicia de los Estados Unidos de América (DoJ), publicó una guía denominada "Investigación En La Escena Del Crimen Electrónico" (*Electronic Crime Scene Investigation)*. Este documento se enfoca sobretodo en la identificación y recolección de la evidencia. Su estructura es:

- Dispositivos electrónicos (los tipos de dispositivos que se pueden encontrar y cuál podría ser la posible evidencia).
- Herramientas para investigar.
- Asegurar y evaluar la escena.
- Documentar la escena.
- Recolección de evidencia.
- Empaque, transporte y almacenamiento de la evidencia.
- Examen forense y clasificación de delitos.
- Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

2.1.2.2.2.4 Guía DoJ 2

Otra guía del Departamento de Justicia de los EEUU, es el "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement). Esta guía está pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es:

- Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.
- Determinar el curso de la evidencia a partir del alcance del caso.
- Adquirir la evidencia.
- Examinar la evidencia.
- Documentación y reportes.
- Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

2.1.2.2.2.5 Mejores Prácticas (Guía Hong Kong)

El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publicó una guía denominada "Computación Forense - Parte 2: Mejores Prácticas" (Computer Forensics – Part 2: Best Practices). Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es:

- Introducción a la computación forense.
- Calidad en la computación forense.
- Evidencia digital.
- Recolección de Evidencia.
- Consideraciones legales (orientado a la legislación de Hong Kong).
- Anexos.

2.1.2.2.2.6 Guía De Buenas Prácticas Para Evidencia Basada En Computadores -Guía Reino Unido-

La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publicó la "Guía de Buenas Prácticas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence). La policía creó este documento con el fin de ser

usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es:

- Los principios de la evidencia basada en computadores.
- Oficiales atendiendo a la escena.
- Oficiales investigadores.
- Personal para la recuperación de evidencia basada en computadores.
- Testigos de consulta externos.
- Anexos (legislación relevante, glosario y formatos)

2.1.2.2.2.7 Guía Para El Manejo De Evidencia En IT (Guía Australia)

Standards Australia (Estándares de Australia) publicó la "Guía Para El Manejo De Evidencia En IT" (Handbook Guidelines for the Management of IT Evidence). Esta guía no está disponible para su libre distribución, sin embargo, para su investigación se consultaron los artículos "Buenas Prácticas en la Administración de la Evidencia Digital" y "New Guidelines to Combat e-Crime", los cuales abordan particularidades de este estándar.

Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital.

Detalla el ciclo de administración de evidencia de la siguiente forma:

- Diseño de la evidencia.
- Producción de la evidencia.
- Recolección de la evidencia.
- Análisis de la evidencia.
- Reporte y presentación.
- Determinación de la relevancia de la evidencia.

2.1.2.2.2.8 Norma ISO/IEC 27037:2012

La norma ISO/IEC 27037:2012 viene a renovar a las ya antiguas directrices RFC 3227, estando las recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales y están más acordes con el estado de la técnica actual. Esta norma está claramente orientada al procedimiento de la actuación pericial en escenario de la recopilación, identificación y posesión de la evidencia digital, no entra en la fase de análisis de la evidencia.

Las tipologías de dispositivos y entornos tratados en la norma son los siguientes:

- Equipos y medios de almacenamiento y dispositivos periféricos.
- Sistemas críticos (alta exigencia de disponibilidad).
- Ordenadores y dispositivos conectados en red.
- Dispositivos móviles.
- Sistema de circuito cerrado de televisión digital.

Los principios básicos en los que se basa la norma son:

Tabla 2.3. Principios de la norma ISO/IEC 27037

Principio	Descripción
Aplicación de Métodos	La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en lo posible obteniendo copias de respaldo.
Proceso Auditable	Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.
Proceso Reproducible	Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

Proceso Defendible	Las herramientas utilizadas deben de ser mencionadas y éstas deben haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

Fuente: http://peritoit.com/2012/10/23/isoiec-270372012

2.1.2.2.3 Preservación de la Evidencia Digital

De suscitarse el caso en que se inicie un proceso jurídico contra los atacantes de un sistema informático, será imperioso registrar de manera clara y exacta como se ha conservado la evidencia posterior a su recopilación mientras se llevaban a cabo las etapas anteriores, por lo tanto es importante fijar los métodos apropiados para el almacenamiento y etiquetado de evidencias. Se sugiere obtener copias exactas de la evidencia conseguida haciendo uso de mecanismos de verificación de integridad de cada copia, las mismas que deberán ser documentadas y adicionadas en el respectivo etiquetado.

De igual forma, el otro factor a sustentar dentro de esta fase es el proceso de la "Cadena de Custodia", en este factor se fijan las responsabilidades y controles de todas las personas que manipulen la evidencia digital; es preciso la elaboración de un registro donde se documenten los datos requeridos tales como: nombres, fechas, custodios, lugar de almacenaje, transporte, etc. Asimismo los datos personales del personal involucrado en el proceso de manipulación de copias, iniciando desde la obtención hasta el proceso de almacenamiento.

2.1.2.2.4 Análisis de la Evidencia

Posterior a que se hayan realizado los procesos iniciales (identificación, recopilación y preservación de las evidencias digitales) se deberá continuar con el Análisis Forense de dichas evidencias, cuyo fin prioritario es el de reconstruir usando todos los datos disponibles, la línea de tiempo en la que se llevó a cabo el ataque, estableciendo la cadena de sucesos desde el punto anterior al inicio del ataque, hasta su hallazgo.

Dicho análisis deberá responder las incógnitas de cómo se llevó a cabo el ataque, por quien o quienes fue realizado, en qué circunstancias se llevó a cabo y qué se buscaba al realizar el ataque (objetivo), de igual forma se deberán reconocer cuáles fueron los daños causados.

Es importante acotar que existen herramientas informáticas que permiten llevar a cabo análisis forense de evidencias digitales, a continuación mencionamos las más destacadas:

- Encase: es un software de investigación forense informática, que tiene la capacidad de realizar análisis complejo de evidencia digital en diversas plataformas, la licencia en la versión *enterprise* es de aproximadamente $4000, entre sus principales características tenemos:

  - ✓ Amplia compatibilidad de formatos disponibles.
  - ✓ Amplia compatibilidad con navegadores disponibles.
  - ✓ Análisis y generación de informes de manera detallada.
  - ✓ Recopilación inteligente de evidencia digital.
  - ✓ Validado por los tribunales de justicia.

- FTK Imager: es una potente herramienta forense enfocada básicamente a la adquisición y tratamiento de imágenes de cualquier dispositivo de almacenamiento, para ser posteriormente usadas como evidencias forenses en un proceso legal.

  - ✓ Obtención (volcado) de la memoria RAM.
  - ✓ Interfaz intuitiva
  - ✓ Potente velocidad de procesamiento
  - ✓ Creación de imágenes bit a bit de discos duros y demás unidades de almacenamiento.
  - ✓ Creación de hashes de archivos y dispositivos (md5 y sha1). El *hash* es la prueba de que los ficheros no se han alterado ni modificado en ningún caso.

- Digital Forensics Framework: Es una herramienta basada en python con un módulo de sistema flexible para investigación forense digital de memorias USB, PDA, tarjetas de memoria y celulares. Entre sus principales características constan:

  - ✓ Recuperación potente de archivos borrados.
  - ✓ Análisis del sistema de archivos de teléfonos móviles
  - ✓ Descifrar contenido y metadatos de SMS para mostrarlos como en un teléfono móvil.

- Easy Recovery Professional: Es una solución para recuperar datos, reparar archivos, correo electrónico y realizar diagnóstico de discos. Posee soporte para:

  - ✓ Discos duros IDE/ATA/SATA/SCSI
  - ✓ Discos extraíbles
  - ✓ Soportes periféricos
  - ✓ Soportes Digitales.

Adicionalmente, existen distribuciones del sistema operativo Linux enfocadas al análisis forense, entre las cuales tenemos:

Tabla 2.4. Distribuciones Linux para análisis forense

Distribución	**Sistema Operativo base**	**Descripción**
Deft Linux	Ubuntu	Su ambiente gráfico de escritorio es LXDE integrando todo un conjunto de aplicaciones open-source y WINE (ésta última para ejecutar las herramientas de Microsoft Windows en Linux).
Caine	Ubuntu	Ofrece un completo ambiente de cómputo forense organizado para integrar todas las herramientas existentes como módulos y proveer todo ello en una interface muy amigable.

Helix Live Forensic	Knoppix	Se centra en la respuesta a incidentes y herramientas forenses. Está destinada a ser utilizada por personas que tienen una buena comprensión de respuesta a incidentes y técnicas forenses.
Kali	Debian	Diseñada principalmente para la auditoría y seguridad informática en general, incluye las herramientas de software libre más populares en materia forense de forma rápida y sencilla.
Santoku	Lubuntu	Herramienta especializada en pruebas de seguridad, análisis de malware y análisis forenses para teléfonos móviles, válida para dispositivos con sistemas operativos android, BlackBerry, IOS y Windows Phone.

Fuente: Los autores

2.1.2.2.5 Documentación y Presentación de Resultados

En esta etapa, el especialista o perito se debe asegurar que todas las fases precedentes se documentaron de forma correcta, esta acción a más de que permite gestionar el incidente, de igual forma permite llevar un mejor control de los procedimientos o mecanismos ejecutados desde el hallazgo hasta la culminación del proceso de análisis forense. Se sugiere considerar los formularios a continuación:

- Formulario de identificación de equipos y componentes.
- Formulario de obtención o recolección de evidencias.
- Formulario para el Control de custodia de evidencias.
- Formulario de incidencias tipificadas.

En esta última fase, se elaboran los informes periciales (técnicos) los cuales deben contener una declaración pormenorizada del análisis realizado, en este documento se deberá describir entre otros aspectos: la metodología, técnicas y el compendio de los hallazgos encontrados.

Es importante destacar que en el Art. 511, inciso sexto, del actual Código Orgánico Integral Penal del Ecuador, el Informe Pericial deberá contener como mínimo lo siguiente:

- Lugar y Fecha de la realización del Peritaje
- Identificación del Perito
- Descripción y estado de la persona u objeto peritado
- Técnica utilizada para la pericia
- Fundamentación científica
- Ilustraciones gráficas, de ser necesarias.
- Conclusiones
- Firma del Perito

El perito podrá dar su versión en el caso que los vestigios del delito hubiesen desaparecido, y opinará si dicha desaparición fue por motivos naturales o intencionales, su testimonio será por solicitud del juez.

2.1.2.3 Auditoría Informática

Otra práctica bien usada por parte de los especialistas informáticos mientras se lleva a cabo el proceso de investigación es la auditoría informática, procedimiento sobre el cual se han creado varios marcos de referencias y conjunto de mejores prácticas para su adecuada aplicabilidad; habitualmente utilizada con el fin de prevenir y detectar fraudes de toda índole de una forma especializada, asimismo este campo ha desarrollado la auditoría forense, la cual es definida por Pedro Lollett como:

> *"El uso de técnicas de investigación criminalística, integradas con la contabilidad, conocimientos jurídicos procesales, y con habilidades en finanza y de negocio, para manifestar información y opiniones como pruebas en los tribunales"* (Lollett, 2007).

2.1.2.3.1 Objetivos de la Auditoría Informática

A continuación se exponen los objetivos que persigue la auditoria informática que son descritos por Alonso Tamayo Alzate en su libro: "Auditoría de Sistemas una Visión Práctica", los cuales se presentan agrupados en objetivos generales y objetivos específicos, de la siguiente forma:

Figura 2.4: Objetivos de la Auditoría de Sistemas

Fuente: (Tamayo, Auditoría de Sistemas una Visión Práctica, 2010)

2.1.2.3.2 Objetivos Generales

- Evaluar las políticas generales de órdenes técnicos con respecto al software, hardware, desarrollo, implantación, operación y mantenimiento de sistemas de información.
- Evaluar las políticas generales sobre seguridad física con respecto a instalaciones, personal, equipos, documentos, back-ups, pólizas y planes de contingencia.
- Evaluar los recursos informáticos de la empresa con énfasis en su nivel de tecnología, producción de software y aplicaciones más comúnmente utilizadas.
- Asesorar a la gerencia y altos directivos de la empresa en lo relacionado con los sistemas de información, de tal forma que el proceso de toma de decisiones se efectúe lo más acertadamente posible.

2.1.2.3.3 Objetivos Específicos

- Evaluar el grado de intervención de la auditoria de sistemas en las etapas de desarrollo, implementación y mantenimiento de las aplicaciones.

- Evaluar las políticas y criterios para la adquisición y/o desarrollo del software, y en la respectiva segregación de funciones para este proceso.
- Administrar los procedimientos administrativos de seguridad informática.
- Evaluar los riesgos y fraudes de mayor incidencia al interior de la empresa.
- Examinar la documentación existente con respecto a los manuales de sistemas, usuario, operación, auditoría, funciones y procedimientos, para determinar su actualización y efectividad.
- Revisar los procedimientos existentes sobre planeación, ambiente laboral, entrenamiento y capacitación, desempeño, supervisión, motivación y remuneración del talento humano.
- Examinar los procedimientos existentes con respecto al software, hardware, desarrollo, implementación, operación y mantenimiento de los sistemas informáticos.
- Revisar los procedimientos existentes sobre seguridad física con respeto a instalaciones, personal, equipos, documentación, back-ups, pólizas y planes de contingencias.
- Control de modificación a las aplicaciones existentes.

En nuestro país, el Organismo de Control que por su naturaleza puede ejecutar acciones de Auditoría Informática de forma autónoma en entidades del sector público, es la Contraloría General del Estado, cuyo ámbito de control le faculta para llevar a cabo programas de auditoría por iniciativa propia.

Según su organigrama, cuenta con un área destinada al apoyo de la Institución como tal (Dirección de las TIC's), mientras que para la ejecución de las auditorías informáticas a los entes públicos cuenta con la Dirección de Auditoría de Tecnologías de la Información (Anexo 1)

2.2 Condiciones Jurídicas en la legislación del Ecuador

Bajo un contexto en que la información es un activo jurídico a proteger, se han promulgado leyes y decretos que determinan especificaciones conforme a la importancia de las tecnologías de la Información, tales como:

1. Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
2. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
3. Ley de Propiedad Intelectual.
4. Ley Especial de Telecomunicaciones.
5. Ley de Control Constitucional (Reglamento Habeas Data)

2.2.1 Ley Orgánica de Transparencia y Acceso a la Información Pública.

Esta ley, publicada en el Registro el 18 de mayo del 2004 y reformada por última vez en el año 2011 (parámetros para la aplicación de los Art. 7 y 12), fue promulgada con el objetivo de llevar a la praxis la disposición contenida en el Art. 81 de la Constitución Política de 1998, en la que se especificaba que “la información es un derecho de las personas que garantiza el Estado”; por otro lado, en la actual Constitución se señala en el Art. 18 lo que "Todas las personas, en forma individual o colectiva, tienen derecho a acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas"

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) desde su origen determina que los Organismos o Instituciones del sector público en su totalidad pongan a disposición de los ecuatorianos, el acceso de forma libre a la información institucional, ya sean estos: estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc., mediante publicaciones en sus respectivos portales web; en este contexto, la Constitución vigente, en el capítulo tercero de las Garantías Jurisdiccionales en las secciones cuarta y quinta acerca de la acción de acceso a la información pública y acción de Habeas Data, también fija estas garantías.

En el Ecuador, el organismo que ejerce vigilancia, controla, analiza y es el encargado de que esta ley se cumpla, es la Defensoría del Pueblo, la misma que en un informe del año 2012 y publicado por diario El Telégrafo, en lo referente al cumplimiento de esta ley, reveló entre lo más relevante lo siguiente:

1. De las 2.500 instituciones registradas por la Defensoría, 1.646 cumplieron al publicar su información dispuesto por la ley
2. El 65.84% entregó a la Defensoría del Pueblo sus informes anuales de transparencia y acceso a la información.
3. La tendencia indica que cada año se supera el porcentaje de cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública LOTAIP. (Diario El Telégrafo, 2012)

En el 2014, el Defensor del Pueblo, Destacó el cumplimiento, en el último año, de la entrega de datos por parte de las instituciones públicas en casi un 100%. (Diario El Universo, 2014)

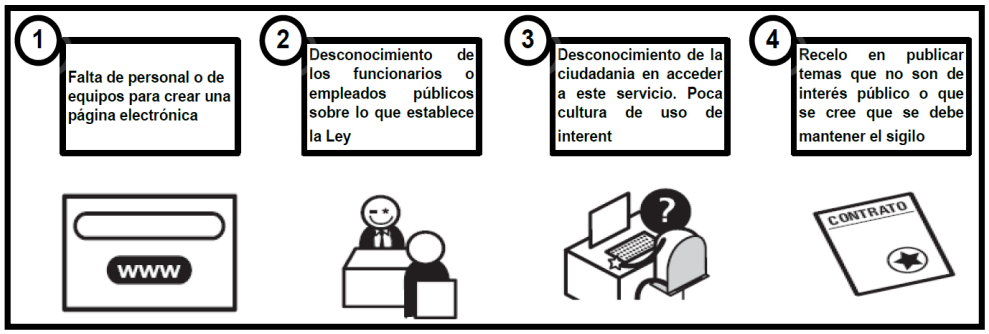


Figura 2.5: Factores que inciden en la poca información pública

Fuente: Defensoría del Pueblo

2.2.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Creada inicialmente el 17 de Abril del 2002 y reformada en el año 2011, procura regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Asimismo, la ley establece que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

La Firma Electrónica es la equivalencia digital de la firma manuscrita, tiene la misma validez legal y se encuentra amparada por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

La firma digital permite la transacción segura de documentos y operaciones en aplicaciones computacionales garantizando los siguientes aspectos:

Tabla 2.5. Características de la Firma digital

Características	Descripción
Identidad	Reconoce unívocamente a un emisor como autor del mensaje.
Integridad	El documento no puede ser alterado de forma alguna durante la transmisión.
No repudio	El emisor no puede negar en ningún caso que un documento no fue firmado.
Confidencialidad	Solo las partes puedan leer el documento (si fuera el caso).

Fuente: Secretaría Nacional de Administración Pública, recuperado de: http://www.administracionpublica.gob.ec/firma-electronica/

Con la firma electrónica pueden realizarse diferentes tipos de transacciones a través de la Internet sin necesidad de desplazarse, ni hacer filas de forma que los trámites públicos se agilitan aumentando la transparencia, lo que se traduce en ahorros significativos de tiempo y dinero. Las aplicaciones de la firma digital son diversas. Se cita algunas de ejemplo a continuación:

- Compras públicas
- Trámites Ciudadanos (Gobierno Electrónico)
- Gestión Documental
- Operaciones Bancarias
- Dinero (pago) Electrónico
- Balances Electrónicos
- Trámites Judiciales y notariales
- Comercio Electrónico
- Facturación Electrónica

2.2.3 Ley de Propiedad Intelectual

La Ley de Propiedad Intelectual promulgada el 19 de Mayo de 1998, surge con el objetivo de ofrecer por parte del Estado una adecuada protección de los derechos intelectuales y obtener la defensa de los mismos, como un elemento necesario para el desarrollo tecnológico y económico del país.

La Institución encargada por la difusión, y ejecución de las leyes de la Propiedad Intelectual en el país es el Instituto Ecuatoriano de Propiedad Intelectual (IEPI); exponer o difundir la importancia que tiene la Propiedad Intelectual en el Ecuador y su respectiva aplicación en los sectores económico, industrial, intelectual y de investigación, no sólo debe ser tarea del profesional del derecho, sino de los industriales y empresarios, de las organizaciones tanto públicas como privadas, de las Instituciones de educación superior e inclusive del propio estado ecuatoriano.

En el más reciente estudio de piratería mundial de software, publicado en el año 2012 y realizado por la Business Software Alliance BSA en el 2011, establece que Ecuador tiene una tasa de piratería de un 68%, lo que constituye un aproximado de pérdidas por 92 millones de dólares y representa un incremento del 16% con respecto a la última medición (79 millones de dólares).

	Tasa de Piratería					Valor Comercial del Software sin licencia ($M)				
	2011	2010	2009	2008	2007	2011	2010	2009	2008	2007
Latino América										
Argentina	69%	70%	71%	73%	74%	$657	$681	$645	$339	$370
Bolivia	79%	80%	80%	81%	82%	$59	$54	$40	$20	$19
Brasil	53%	54%	56%	58%	59%	$2,848	$2,619	$2,254	$1,645	$1,617
Chile	61%	62%	64%	67%	66%	$382	$349	$315	$202	$187
Colombia	53%	54%	55%	56%	58%	$295	$272	$244	$136	$127
Costa Rica	58%	58%	59%	60%	61%	$62	$55	$33	$24	$22
Ecuador	68%	67%	67%	66%	66%	$92	$79	$65	$37	$33
El Salvador	80%	80%	80%	80%	81%	$58	$55	$46	$28	$28
Guatemala	79%	80%	80%	81%	80%	$116	$106	$74	$49	$41
Honduras	73%	73%	74%	74%	74%	$24	$22	$17	$9	$8
México	57%	58%	60%	59%	61%	$1,249	$1,199	$1,056	$823	$836
Nicaragua	79%	79%	79%	79%	80%	$9	$8	$5	$4	$4
Panama	72%	72%	73%	73%	74%	$74	$68	$42	$24	$22
Paraguay	83%	83%	82%	83%	82%	$73	$55	$29	$16	$13
Peru	67%	68%	70%	71%	71%	$209	$176	$124	$84	$75
República Dominicana	76%	76%	77%	79%	79%	$93	$87	$66	$43	$39
Uruguay	68%	69%	68%	69%	69%	$85	$78	$40	$25	$23
Venezuela	88%	88%	87%	86%	87%	$668	$662	$685	$484	$464
tros de LA	84%	84%	83%	84%	83%	$406	$405	$430	$319	$195
TOTAL LA	61%	64%	63%	65%	65%	$7,459	$7,030	$6,210	$4,311	$4,123

Figura 2.6: Estudio Anual de Piratería Mundial de Software

Fuente: http://globalstudy.bsa.org/2011/downloads/translated study/2011GlobalPiracyStudy_es.pdf

Las decisiones tomadas para la protección de las especificaciones de propiedad intelectual y de los derechos de autor se han elaborado por iniciativas de la BSA tales como “Marca el Límite”, “Buenos Negocios”, “Evite riesgos, use software legal” las cuales buscan incentivar el uso de software legal. Adicionalmente, una campaña impulsada por la Business Software Alliance es la habilitación del portal “Reporte confidencial sobre piratería de software”, en el cual se permite denunciar de manera confidencial la piratería del software en Latino América.

Abordar acerca de la propiedad intelectual es también reconocer, que entre los problemas prioritarios que enfrenta esta rama jurídica moderna, se encuentra la piratería e imitación de las obras del intelecto humano, las cuales conllevan graves consecuencias económicas y sociales; adicional a los perjuicios de los dueños de derechos de propiedad intelectual, pues esta pérdida no solo afecta a los fabricantes de los productos pirateados, sino a la disminución de ingresos tributarios y aún más a la pérdida de empleos, afectando la vitalidad social y financiera del país.

2.2.4 Ley Especial de Telecomunicaciones

La Ley Especial de Telecomunicaciones fue publicada inicialmente el 10 de Agosto de 1992, y recientemente reformada en el 2014, expresa que es imprescindible proveer a los servicios de telecomunicaciones de una normativa jurídica afín a la importancia, complejidad, volumen y especialidad de dichos servicios, de igual forma, ofrecer una adecuada regulación y propagación de los sistemas radioeléctricos, y servicios telemáticos.

Esta ley reconoce los derechos de los usuarios para que obtengan un servicio de calidad, además que se ordena una estructura legal que estaba dispersa y que promovió la duplicidad de esfuerzos de la norma.

Esta nueva Ley de Telecomunicaciones tiene como propósito desarrollar el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado, que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos.

Uno de los cambios planteados es que la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) reemplazará a la SUPERTEL (Superintendencia de Telecomunicaciones). Esta nueva entidad será la encargada de controlar las tarifas a través de techos establecidos, así como impedir el redondeo en las tarifas telefónicas.

Esta ley posee varios aportes de la normativa especificada por la Unión Internacional de Telecomunicaciones UIT, entre ellas mencionamos las siguientes: Servicios de Transmisión de Datos, límite de precios, contratos de concesión, Licencias, Interconexión, entre otras.

2.2.5 Ley Orgánica de Control Constitucional

La Ley Orgánica de Control Constitucional, fue reformada en el año 2009 y fue calificada con jerarquía y carácter de Ley Orgánica, por resolución legislativa, publicado en Registro Oficial el 22 de Octubre del 2009.

La Ley Orgánica de Control Constitucional, en su Capítulo VI del Habeas Data establece que el objetivo de esta figura legal es "garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.".

En la actual Constitución del Ecuador, en su capítulo tercero acerca de las Garantías Jurisdiccionales de su sección quinta, Art. 92 sobre la acción de Habeas Data, también se fija el recurso jurídico del Habeas Data.

De igual manera, existen normativas relacionadas que han sido establecidas en el actual COIP, las cuales se abordarán en el Capítulo 4 con mayor profundidad.

Se ha abordado la conceptualización de los delitos informáticos, el estudio de su elemento principal, la evidencia digital, así como los procedimientos existentes para su respectivo análisis e investigación; es preciso señalar que los profesionales destinados al esclarecimiento de actos indebidos en los que se hace uso de medios tecnológicos, estén al tanto de los avances relacionados con esta materia de aplicación, y así mantenerse aptos para reaccionar de forma adecuada frente a actos llevados a cabo por la delincuencia informática.

CAPÍTULO III

PERITOS FORENSES INFORMÁTICOS

3.1 El Perito

En el libro de Juan Carlos Riofrío, La Prueba Electrónica, el autor conceptualiza al perito de la siguiente manera:

> *"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 y así aclarar el asunto litigioso en revisión."*(Riofrío, 2004)

Es así que bajo esta definición, el perito es un auxiliar de la justicia, que no tiene como objetivo resolver un problema operativo, sino revelar o explicar la causa y los motivos de dichos problemas, posterior a un análisis y estudio exhaustivo.

De igual forma, el especialista en informática forense Emilio del Peso Navarro, en su publicación editorial, Peritajes Informáticos, contribuye con una definición para el término de perito informático:

> *"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."*(Del Peso, 2001)

Por lo tanto, considerando esta definición, al ser el perito informático un especialista que emitirá un criterio u opinión, la misma que deberá estar apoyada tanto en la parte técnica como científica, logre determinar conclusiones objetivas e imparciales sobre un acontecimiento, y no solo fundamentarse con impresiones u opiniones.

De acuerdo a lo contemplado en el Reglamento del Sistema Pericial Integral de la Función Judicial en su Art. 3 y publicado mediante resolución 040-2014 en abril del 2014, indica que: "Todo perito que sea designado como tal en cualquier tipo de proceso judicial o pre procesal, debe estar previamente calificado por el Consejo de la Judicatura, y debe cumplir con las regulaciones y la normativa de la resolución".

El parágrafo tercero del actual COIP indica que: "De no existir persona acreditada como perito en determinadas áreas, se deberá contar con quien tenga conocimiento, especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje. Para los casos de mala práctica profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organismo rector de la materia".

Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados como prueba, a través de testimonios anticipados o podrán ser receptados mediante video conferencias de acuerdo a las reglas del Código Orgánico Integral penal del Ecuador.

El Consejo de la Judicatura, mantiene el registro de los profesionales calificados a nivel nacional en el cual existen alrededor de 1000 peritos acreditados en diferentes ramas como: la Criminalística, Medicina humana, Aduana, Lavado de Activos, Traducciones, entre otras, incluido los peritos en la rama de informática y telecomunicaciones.

Consecuentemente existen 94 subespecialidades dentro de las áreas de estudio descritas anteriormente, entre ellas: Genética, Avalúos, Psicología Criminal, Explosivos, Odontología Forense, Joyería, Dactiloscopía, grafología, entre otras. (ver Anexo 2)

Del reporte que se encuentra en el portal web del Consejo de la Judicatura relacionado a los especialistas calificados, generamos el siguiente gráfico que muestra con valores porcentuales (relativos) la cantidad de peritos que existen por cada una de las especialidades.

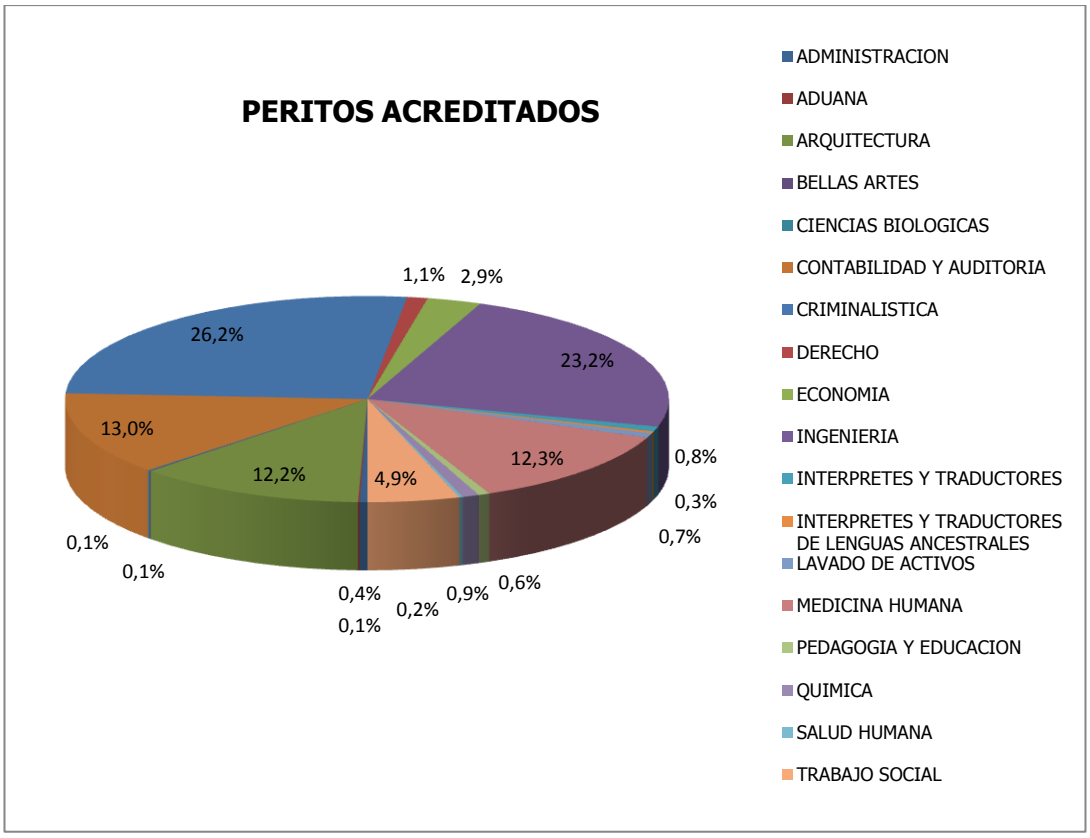


Figura 3.1: Peritos acreditados por especialidad en Ecuador

Fuente: Consejo de la Judicatura

En lo concerniente a los peritos informáticos y de telecomunicaciones en el país, al mes de Febrero del 2015, están calificados 11 profesionales como peritos (9 profesionales de la rama de informática y 2 profesionales de la rama de Telecomunicaciones), lo que representa el 1.1% del total de especialistas acreditados en todo el país. (Ver Anexo 3)

En el Artículo 511 del Actual COIP se especifica que las y los peritos deberán:

Tabla 3.1. Reglas Generales de Obligaciones de los Peritos

Reglas Generales	
1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.	2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.
3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este	4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito

Código para las o los juzgadores.	que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.
5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.	6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.
7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.	8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por estas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.

Fuente: Código Orgánico integral Penal del Ecuador

3.1.1 Perfil del Perito

En varias de las publicaciones realizadas por Jeimy Cano, Phd. Acerca del perfil requerido por parte de un perito informático, manifiesta lo siguiente:

> *"Un perito informático 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".* (Cano J. , 2006)

Por lo manifestado anteriormente, es preciso que el perito informático certifique experiencia, conocimientos tanto teóricos como prácticos, destrezas en la aplicación de procedimientos y técnicas, y que sus informes sean presentados de manera procedimental y estructural.

Para las investigaciones o análisis forenses aplicables a la informática, se demandan de especialistas con altos conocimientos en las TIC's, alineados a la ejecución de procedimientos científicamente validados y reconocidos sobre las evidencias

digitales sujetas de estudio; para ellos existen certificaciones profesionales de carácter internacional que pueden ser sujetas de estudio, certificación y aplicación por los profesionales informáticos.

Con el objetivo de complementar el perfil del profesional informático forense, existen instituciones internacionales tales como la EC–Council, International Association of Computer Investigative Specialist (IACIS), High Technology Crime Network (HTCN), Association of Certified Fraud Examiners (ACFE), que en este contexto han elaborado programas de certificación aplicables a la informática forense y seguridad informática, las cuales logran desarrollar destrezas y capacidades en los peritos informáticos para la investigación de un hecho; la siguiente tabla muestra algunas certificaciones de este tipo:

Tabla 3.2. Certificaciones Forenses y de Seguridad Informática.

TIPO	CERTIFICACIÓN	ORGANIZACIÓN
Forense	CHFI – Computer Hacking Forensic Investigator	EC-Council
	CCCI – Certified Computer Crime Investigator	HTCN
	CCE – Certified Computer Examiner	ACFE
	CFE – Certified Fraud Examiners	ACFE
	CFEC - Computer Forensic External Certification	IACIS
Seguridad Informática	CFA – Computer Forensic Analysis	WISE
	CCI – Computer Crime Investigator	EC-Council
	CEH – Certified Ethical Hacker	EC-Council
	CHFI – Computer Hacking Forensic Investigator	EC-Council

Fuente: Los Autores

Por lo general, las certificaciones descritas en la tabla anterior, exigen a los especialistas informáticos que desarrollen habilidades en:

1. Identificación y recolección de evidencias en medios magnéticos.
2. Comprensión y práctica en procedimientos de revisión y análisis forenses.
3. Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática.

4. Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.
5. Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación.
6. Comprensión de los diferentes sistemas de archivos asociados con sistemas operativos, acceso a archivos temporales, de caché, de correo electrónico, etc.
7. Conducir de manera detallada, recuperación de datos de todas las particiones de un disco.
8. Comprensión de técnicas de rompimiento de contraseñas y claves de seguridad.

Cabe recalcar, que el perito debe poseer, adicional a sus amplios conocimientos, altos valores éticos, morales y profesionales (deontología), que avale la seriedad de su acreditación ante un proceso jurídico en que se hayan solicitado de sus conocimientos y habilidades para el análisis de un acto ilícito que haya ocurrido.

Posterior a que haya finalizado el proceso de investigación por parte del perito informático, y después de haber entregado su informe, el mismo podrá ser convocado por la autoridad pertinente, para explicar o ampliar su informe, ya sea de manera escrita u oral, para aquello, deberá poder transmitir lo que ha realizado y analizado dentro de su investigación pericial, deberá justificar ante el juez, fiscal, o tribunal, el o los motivos del por qué se le debe creer en lo referente a sus conclusiones, las herramientas o técnicas que ha usado en el lapso del proceso de investigación e inclusive, podría indagarse acerca de los procedimientos y técnicas ejecutadas en su análisis. El perito no podrá hacer uso de herramientas forenses de software crackeadas, ya que esta acción constituye una causal para la invalidez del informe presentado.

3.1.2 Requisitos de acreditación de Peritos

Para poder ser calificado como perito en el Consejo de la Judicatura, es preciso cumplir con varios requisitos según lo dispuesto en el Art. 4 de la Resolución 040-2014, los cuales son:

1. Ser mayores de edad, ser capaces y estar en ejercicio de sus derechos de participación
2. Ser conocedoras o conocedores y/o expertos en la profesión, arte, oficio, o actividad para la cual soliciten calificarse.
3. En el caso de profesionales, tener al menos dos años de graduadas o graduados a la fecha de solicitud de calificación, y cumplir con los requisitos de experiencias establecidos en este reglamento. Para las y los demás expertos tener al menos dos años de práctica y experiencia a la fecha de la solicitud de calificación, en el oficio, arte o actividad en la cual tengan interés de calificarse.
4. También se podrán presentar, para justificar la experticia y conocimiento de la o el solicitante, hasta diez informes periciales realizados en los últimos dos años, los cuales serán analizados por el Consejo de la Judicatura para determinar si acreditan experticia; y,
5. No hallarse incursas o incursos en las inhabilidades o prohibiciones para ser calificada o calificado como perito previstas en la ley y este reglamento.

3.2 Acreditación de Peritos

En el Reglamento del Sistema de Acreditación de Peritos publicado el 7 de Junio del 2013, se establece que el certificado de acreditación será conferido por las Directoras o Directores Provinciales y contendrá:

1. Nombres y apellidos completos del perito;
2. Número de cédula de ciudadanía o pasaporte, según el caso;
3. Número de inscripción o acreditación;
4. Tiempo de vigencia; y,
5. Título universitario o Certificación en la práctica de arte u oficio y materia de especialidad.

Este certificado deberá ser presentado ante la autoridad respectiva de la Función Judicial, en el momento de la posesión del cargo para la realización de la pericia.

El tiempo de vigencia del certificado, así como de la inscripción, será de dos años; y podrá renovarse por el mismo periodo.

En cuanto a las designaciones de los peritos, se deberán respetar los principios de profesionalidad, especialidad, imparcialidad y alternabilidad, para cuyo efecto los jueces los designarán a través del módulo de peritos del sistema SATJE; en los casos en los que no se cuente con el perito requerido en un determinado cantón, el sorteo se realizará del listado del cantón más cercano. La Fiscalía los escogerá del listado constante en la página web del Consejo de la Judicatura conforme a los procedimientos internos que rijan en dicha entidad.

3.2.1 Organismos Facultados para la Acreditación de peritos

De acuerdo a lo establecido en el Reglamento para el Sistema de Acreditación de Peritos, "El servicio pericial debe ser organizado y controlado por el Consejo de la Judicatura, por lo que de conformidad con el Art. 264 numeral 14 del código de la Función Judicial, a este órgano le corresponde acreditar y sistematizar un registro de los peritos autorizados y reconocidos como idóneos, cuidando que estos sean debidamente calificados y acrediten experiencia y profesionalización suficiente." Por lo antes mencionado, El Consejo de la judicatura es el único ente que puede acreditar y nombrar peritos.

En años anteriores previo a la publicación de la Resolución 040-2014 en la que se definía al Consejo de la Judicatura, existían Instituciones que calificaban a peritos para procesos específicos a su área de aplicación, entre ellos tenemos: Centros de Conciliaciones y Arbitraje, Cámaras de industrias, el Instituto Ecuatoriano de Propiedad Intelectual, El Ministerio Público y hasta la Superintendencia de Bancos.

3.2.2 Documentos y Anexos a presentarse

Las personas que deseen ser certificadas o calificados como peritos del Consejo de la Judicatura, según el Art. 6 del Reglamento, deberán adjuntar los siguientes formularios, documentos y anexos:

1. Solicitud de Calificación, Formulario 1 situado en el portal web www.funcionjudicial.gob.ec
2. Hoja de Vida, Formulario 2 situado en el portal web www.funcionjudicial.gob.ec
3. Copia de: Certificados de Experiencias avalado por Instituciones públicas o privadas, cualquier otro documento que acredite sus conocimientos o experticia.
4. Para los extranjeros, copia certificada por notario de las páginas de identificación del pasaporte, cédula de identidad y/o de la visa, a más de los requisitos de experiencia y capacitación legalizados.
5. Comprobante de pago no reembolsable, del precio público por servicios administrativos.
6. Declaración Juramentada ante notario, Formulario 3 situado en el portal web www.funcionjudicial.gob.ec, en el que declarará bajo juramento, que:

    a) No ha recibido sanción por perjurio, lesa humanidad, odio, etc.
    b) No ha recibido sanción por un delito sancionado con pena de privación de libertad durante el último año.
    c) No se encuentre inhabilitado para ejercer una función pública.
    d) Se encuentre al día en sus obligaciones tributarias con el S.R.I.
    e) No ha incurrido en falsedad, adulteración o inexactitud de los datos incluidos en los formularios de postulación.
    f) Se somete a las disposiciones establecidas en este reglamento.
    g) Que conoce el Reglamento del Sistema Pericial Integral de la función Judicial.
    h) Las personas postulantes autorizarán al CNJ para que sus datos puedan ser verificados de acuerdo a los datos consignados.

3.2.3 Honorarios de Peritos

En el capítulo VI del Reglamento del Sistema Pericial Integral se aborda todo lo relacionado a los honorarios que recibirán los peritos acreditados por las funciones realizadas, donde se indica textualmente que: "Los peritos tienen derecho de percibir honorarios por la actividad pericial que desarrollen dentro de los procesos judiciales

y/o pre procesales, los cuales serán cancelados por el Consejo de la judicatura, la Fiscalía General del Estado, o por las partes interesadas, según sea el caso y de conformidad con las disposiciones de la ley y este reglamento."

El valor de los honorarios de los peritos será cancelado de la siguiente forma:

1. El 80% del honorario establecido, hasta quince días después de la fecha de presentación oportuna del informe pericial (Ver Anexo 4); y
2. El 20% del honorario establecido, hasta quince días después del momento del cumplimiento total de todas las otras obligaciones del perito, en donde se incluyen la defensa y/o explicación del informe en audiencias orales, de prueba o de juicio, siempre que esta actividad lo disponga la ley procesal correspondiente.

Los peritos recibirán sus honorarios de conformidad en base a la tabla y criterios establecidos por el Consejo de la Judicatura (Ver Anexo 5). En nuestro caso específico para un perito informático acreditado, sus honorarios fluctúan desde $177 hasta $3540, dependiendo de la complejidad del análisis.

Tabla 3.3: Honorarios de un perito informático

Áreas y Especialización	Actividad	Honorarios
INGENIERIA: ingeniería informática o de sistemas, telecomunicaciones, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 del reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.

Fuente: Reglamento del Sistema Pericial Integral de la Función Judicial

3.2.4 Causales para pérdidas de credenciales de peritos

El Reglamento del Sistema Pericial Integral de la Función Judicial, en su capítulo IX Art.43, establece que, el Consejo de la Judicatura está facultado a retirar la calificación del perito por los siguientes motivos:

- Por comprobarse conforme a derecho inexactitud manifiesta, falsedad o adulteración en los datos y/o documentos entregados para la calificación, o su renovación.
- Por comprobarse violación, y/o no cumplimiento de algunas de las obligaciones generales de todo perito establecidas en el Art.18 de este reglamento.
- No concurrir injustificadamente a las posesiones y/o no aceptar el encargo para el que fue designado dentro del plazo establecido por los jueces, o por las y los fiscales, más de tres veces en un mismo año calendario. Sólo se aceptarán como excusa válida las determinadas en el numeral 1 del Art. 19 del reglamento.
- Renunciar injustamente al encargo para el que fue designada o designado, más de dos veces en un mismo año calendario. La renuncia solamente se justificará por temas provocados por casos fortuitos o fuerza mayor, debidamente comprobados; en caso de enfermedad, para justificarla se presentarán las certificaciones otorgadas y/o validas por el IESS o el Ministerio de Salud.
- Cuando se comprobare conforme a derecho que el informe pericial, o sus ampliaciones, aclaraciones o complementos, fueron realizados y/o expuestos distorsionados los hechos, o las conclusiones de forma intencional con el fin de favorecer indebidamente un criterio o conclusión, o existe error esencial.
- No presentar injustificadamente el informe pericial dentro de los plazos otorgados para el efecto.
- No presentar injustificadamente las ampliaciones, aclaraciones o complementos del informe pericial, dentro del plazo ordenado por la autoridad competente.
- No concurrir injustificadamente a explicar y/o defender el informe pericial en las audiencias orales, de prueba o de juicio para las cuales fueren convocadas o convocados y/o notificadas o notificados.
- Cobrar y/o percibir valores correspondientes a honorarios y/o gastos, diferentes a los establecidos por la jueza o el juez, o la o el fiscal de conformidad con este reglamento.

- No adjuntar ni presentar en el proceso judicial o pre procesal, en todos los casos, la copia certificada de la factura de honorarios autorizada por el Servicio de Rentas Internas.
- No aprobar el Curso Básico de Peritos dentro de los plazos establecidos por este reglamento.

Los peritos que se encuentren inmersos en las actuaciones determinadas en los numerales 3, 4, 6, 7, 8 y 10 del artículo anterior, no podrán renovar su calificación en el plazo de dos (2) años.

3.2.5 Implicaciones Legales para el Perito

El perito que esté calificado, tendrá que estar al tanto de las consecuencias legales que conllevaría el ejercicio de su trabajo en un proceso litigioso, ya que en el inciso 4to. Del Art. 511 del actual COIP indica literalmente que "Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada"

El Art. 572 del COIP, establece que las causas de excusa y recusación son las siguientes:

1. Ser cónyuge, pareja en unión de hecho o pariente dentro del cuarto grado de consanguinidad o segundo de afinidad de alguna de las partes, de su representante legal, de su mandatario o de sus defensores.
2. Ser acreedor, deudor o garante de alguna de las partes, salvo cuando sea de las entidades del sector público, de las instituciones del sistema financiero o cooperativas. Da lugar a la excusa o recusación establecida en este numeral solo cuando conste el crédito por documento público o por documento privado reconocido o inscrito, con fecha anterior al juicio.
3. Tener juicio con alguna de las partes o haberlo tenido dentro de los dos años precedentes si el juicio es civil y cinco años si el juicio es penal. La misma regla se aplicará en el caso de que el juicio sea con su cónyuge, pareja en unión de hecho o pariente dentro del cuarto grado de consanguinidad o segundo de afinidad.

4. Tener interés personal en la causa por tratarse de sus negocios, de los de su cónyuge, pareja en unión de hecho o de sus parientes dentro del cuarto grado de consanguinidad o segundo de afinidad.
5. Ser asignatario, donatario, empleador o socio de alguna de las partes.
6. Intervenir en el proceso como parte, representante legal, apoderado, juzgador, defensor, fiscal, acusador, testigo o intérprete.
7. Tener amistad íntima o enemistad manifiesta con alguno de los sujetos procesales.
8. Tener vínculo con las partes, la víctima o sus defensores por intereses económicos.

Dentro del COIP se establecen algunas implicaciones legales para los peritos, entre ellas tenemos que en el Art. 292 acerca de la Alteración de Evidencias y elementos de prueba se menciona que "La persona o la o el servidor público, que altere o destruya vestigios, evidencias materiales u otros elementos de prueba para la investigación de una infracción, será sancionado con pena privativa de libertad de uno a tres años".

De igual forma en lo que respecta a la Reserva de la Investigación, en el Art. 584 se indica que "Cuando el personal de las instituciones involucradas, los peritos, traductores, intérpretes, que han intervenido en estas actuaciones, divulguen o pongan de cualquier modo en peligro el éxito de la investigación o las difundan, atentando contra el honor y al buen nombre de las personas en general, serán sancionados conforme con lo previsto en este Código".

CAPÍTULO IV

ANÁLISIS DE LOS NUEVOS DELITOS INFORMÁTICOS EN EL ACTUAL COIP E INICIATIVAS GUBERNAMENTALES

4.1 Antecedentes

El acceso a las TIC's en el Ecuador se incrementaron de forma considerable en los últimos años. Según el INEC, en el año 2006, sólo el 6% de los ciudadanos registraba un servicio de internet y a septiembre de 2013 se incrementa en un 65%, es decir, más de 10 millones de ecuatorianos cuentan con acceso a la red.

En la última publicación oficial de resultados estadísticos por parte del Instituto Nacional de Estadísticas y Censos, realizada en el año 2013, se evidencia una considerable reducción de la brecha digital por parte de los ecuatorianos.

Según los resultados del Instituto Nacional de Estadísticas y Censos, la provincia con mayor acceso a internet es Pichincha con el 53,1%, mientras que Los Ríos con el 25,0% es la provincia con menor acceso.

Asimismo, el estudio evidencia que el 32,0% de las personas usó Internet como fuente de información, mientras el 31,7% lo utilizó como medio de educación y aprendizaje.

De las personas que usan Internet, el 45,1% lo hace en su hogar. En el área urbana el mayor porcentaje de la población utiliza Internet en el hogar con el 50,9%, mientras el mayor porcentaje de población del área rural lo usa en centros de acceso público con el 42,5%.

Este incremento en el uso de las Tecnologías de Información fundamentalmente es debido a una ambiciosa política pública del Estado Ecuatoriano a través del Gobierno

Nacional para universalizar su acceso. La disminución del costo del kilobyte de $0.60 en el año 2007, a menos de un centavo, por ejemplo, es una de estas medidas.

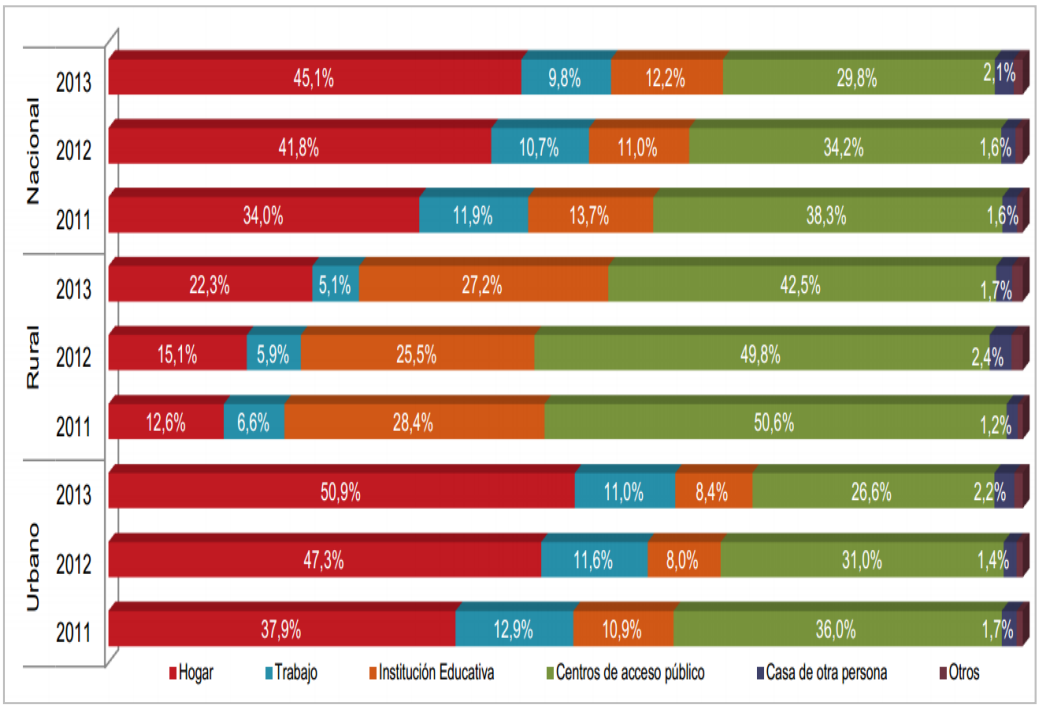


Figura 4.1: Lugar de Uso de Internet por Área

Fuente: Instituto Nacional de Estadísticas y Censos

La tasa de crecimiento en Ecuador, en el uso y acceso a internet, es la más rápida de la región con tasa anual de crecimiento de 38.77 por ciento; Colombia 24.19 por ciento, Chile 9.55 por ciento y Argentina 17.94 por ciento.

Pero el empleo de las TIC's trae también consigo su uso con fines ilícitos. Por los daños ocasionados mencionaremos los acontecimientos más representativos en un contexto global: el caso ocurrido en los Estados Unidos, cuando en 2009 una serie de ataques cibernéticos tuvieron como objetivo la Casa Blanca, el Departamento de Seguridad Interna, el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio; un incidente afín fue reportado por la Guardia Civil de España, en el año 2010, cuando fue desmantelada una de las mayores redes de computadores con más de 13 millones de direcciones IP infectadas y distribuidas en 190 países.

Según la ITU por su siglas en inglés (Unión Internacional de Telecomunicaciones), los ataques cibernéticos en el mundo aumentaron en un 30 por ciento entre 2011 y 2012 y, en el año 2014, 550 millones de personas han sido afectadas, generando pérdidas económicas en alrededor de 110 mil millones de dólares.

El delito informático en Ecuador fue de total relevancia desde que en 1999 se abordó el tema de la discusión del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, en el país se empezaron a dictar cursos, seminarios, se conformaron comisiones para el debate de la Ley y para que se formulen consideraciones, es aquí donde organismos que se encontraban directamente interesados como el CONATEL, la SBS, las Cámaras de Comercio y otras entidades que ya consideraban al comercio electrónico como una excelente oportunidad para realizar negocios y así lograr que el país esté dentro de este nuevo auge.

Como es de suponer, cuando la ley se propuso en un inicio, tenía un gran número de falencias, que con el tiempo se fueron mejorando, entre ellas la parte penal de dicha ley; por lo que las contravenciones a la misma es decir los delitos informáticos, se castigarían de acuerdo a lo establecido en nuestro Código Penal, el cual ya contaba con 70 años de creado, es así que los tipos penales allí presentes, no consideraban los nuevos adelantos de la informática por lo que provocaba relativamente inútil dar seguridad al comercio electrónico ante el acecho del crimen informático.

Ya en abril del 2002 y posterior a las innumerables discusiones entre los diputados, la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas fue aprobada; y por lo tanto, las reformas al Código Penal que sancionaban a los denominados Delitos Informáticos.

Anteriormente en el país no existían unidades especializadas de investigación que traten casos de delitos informáticos, debido a esta debilidad se han creado hasta el momento dos Unidades Especializadas relacionadas al delito informático y al análisis forense, estas son: la Unidad de Investigación del Cibercrimen de la Policía Judicial del Ecuador y el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado respectivamente.

4.1.1 Unidad de Investigación de Delitos Tecnológicos de la Policía Judicial del Ecuador

De acuerdo a lo comunicado por el Ministerio del Interior mediante su portal digital, La Policía Nacional creó en enero del 2012 una Unidad de Investigación de Cibercrimen. Cuyo objetivo es el de detectar, identificar, localizar y neutralizar el accionar de personas con estas conductas ilícitas, a través del uso de la tecnología. En el caso de que cualquier ciudadano requiera la colaboración de los agentes de este departamento deberá acudir a la Fiscalía, para que la Policía Judicial derive su proceso a uno de sus expertos informáticos.

Figura 4.2: Escudo de la UIDT - Policía Judicial
Fuente: Fiscalía General del Estado.

Para el Coronel Nicolay Zapata, Jefe de la Unidad de Investigación de Delitos Tecnológicos de la Policía Judicial, "el Cibercrimen organizado cambió su modus operandi, dejó de clonar tarjetas de crédito y débito para enfocarse en Internet para robar. Su propósito es conseguir más dinero electrónico y afectar a más usuarios"

Esta declaración fue hecha en el 2013 por Zapata ante la Comisión de Justicia de la Asamblea Nacional para pedir la tipificación de siete delitos cibernéticos dentro del Código Integral Penal.

El Myr. Nicolay Zapata reveló que el robo de información de tarjetas en locales o en cajeros se ha reducido en el país. No obstante, los robos por medio de phishing, troyanos, virus informáticos han incrementado.

4.1.2 Departamento de Delitos Informáticos y Análisis Forense de la Fiscalía General Del Estado.

El Fiscal General Del Estado creó mediante Acuerdo 104-FGE-2008 el Departamento de Delitos Informáticos y Análisis Forense de la FGE en el año 2008, esto con el fin de proteger a los usuarios de internet frente al progresivo avance de la criminalidad informática, que explota las vulnerabilidades de los sistemas informáticos y ante la urgente obligación de extender especial protección a los menores, que sufren una mayor indefensión frente a delitos como la pornografía infantil.

El departamento tiene el objetivo principal de ser una ayuda en cuanto a la investigación y persecución de la criminalidad informática en todos sus aspectos y ámbitos, y con mayor intensidad en:

- Amenazas, injurias, calumnias por correo electrónico, SMS, tablones de anuncios, foros, newsgroups, Web, etc.
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones: Bypass.
- Fraudes en Internet. Fraude Informático, Uso fraudulento de tarjetas de crédito, Fraudes en subastas. Comercio electrónico.
- Seguridad Lógica. Virus. Ataques de denegación de servicio. Sustracción de datos. Terrorismo Informático.
- Hacking. Descubrimiento y revelación de secreto. Suplantación de personalidad, Interceptación ilegal de comunicaciones.
- Sustracción de cuentas de correo electrónico.

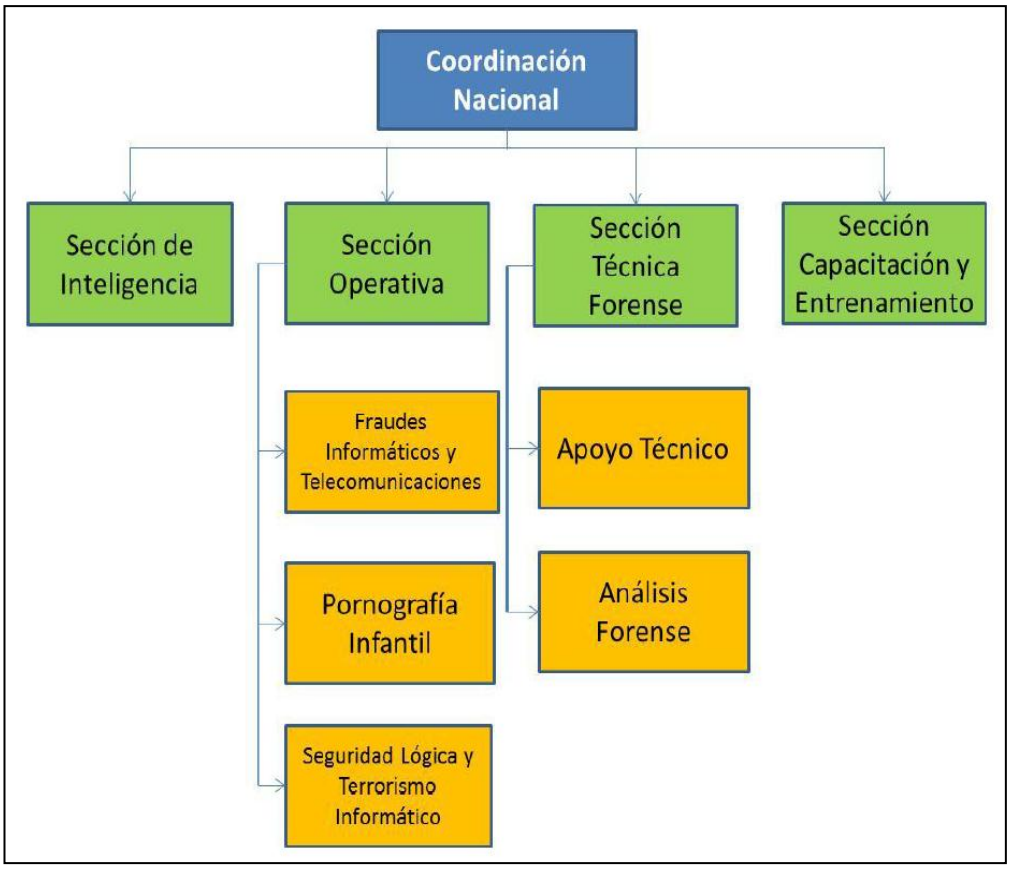


Figura 4.3: Estructura de la Unidad de Delitos Informáticos y Análisis Forense

Fuente: Fiscalía General del Estado.

4.1.2.1 Funciones del Departamento de Análisis Forense

1. Asesorar a todas la Unidades Operativas de la Fiscalía General del Estado a Investigar y perseguir a nivel procesal y pre procesal penal toda infracción que utilice a la informática como medio o fin para la comisión de un delito en especial todo lo relacionado al fraude informático, acceso no autorizado a sistemas de información, pornografía infantil, interceptación de comunicaciones entre otros.
2. Desarrollar en los miembros del Departamento los conocimientos técnicos 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. Contribuir a la formación continua de los investigadores; la colaboración con la Dirección Nacional de Investigaciones de la Fiscalía General del Estado y de las más importantes instituciones públicas y privadas; la participación activa en los foros internacionales de cooperación con los diferentes Ministerios Públicos, Fiscalías y las unidades policiales especializadas, además de la colaboración con la ciudadanía.
4. Formar y mantener alianzas con las Unidades Especiales de investigación de los Delitos Informáticos a nivel internacional, a fin de obtener su apoyo y soporte en esta clase de investigaciones.
5. Desarrollar una Política de Seguridad Informática General, a fin de prevenir y solucionar cualquier ataque a la integridad y fiabilidad de los sistemas informáticos de entidades públicas y privadas.
6. Implementar a nivel nacional el Sistema Información de Delitos Informáticos mediante el uso del Internet, el cual permitirá a todos los miembros de la Fiscalía obtener información sobre los Delitos Informáticos, su forma de combate y prevención.
7. Promover nuevos canales de comunicación y trabajo con las distintas estructuras y organizaciones gubernamentales implicadas en la lucha contra el fenómeno de la delincuencia informática, para buscar soluciones que permitan alcanzar los niveles de seguridad necesarios para el normal desarrollo de la Sociedad de la Información.

Información obtenida por parte del Director del Departamento de Delitos Informáticos y Análisis Forense de la Fiscalía General Del Estado, Dr. Santiago Acurio, mediante publicación de boletín electrónico por parte de esta Institución.

4.2 Denuncia de Delitos Informáticos en el Ecuador

Cada día son más las personas que optan por realizar transacciones financieras de forma online, ya que se concretan por lo general en tiempo real, son más rápidas, se evitan las colas en los bancos. Inclusive algunas compras tienen un mayor descuento al hacerlas de forma online. Con todo lo mencionado, si no tomamos medidas de seguridad, estas acciones pueden conllevar a consecuencias lamentables.

En la Fiscalía de Pichincha, semanalmente se receptan entre 6 y 10 denuncias sobre delitos informáticos, que consisten en la revelación ilegal de base de datos, su interceptación, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos y los accesos no consentidos a un sistema telemático o de telecomunicaciones. Las noticias del delito en estos casos son conocidos por la Unidad de Patrimonio Ciudadano, donde se proporciona asesoría jurídica a las personas que han sido víctimas de estos delitos.

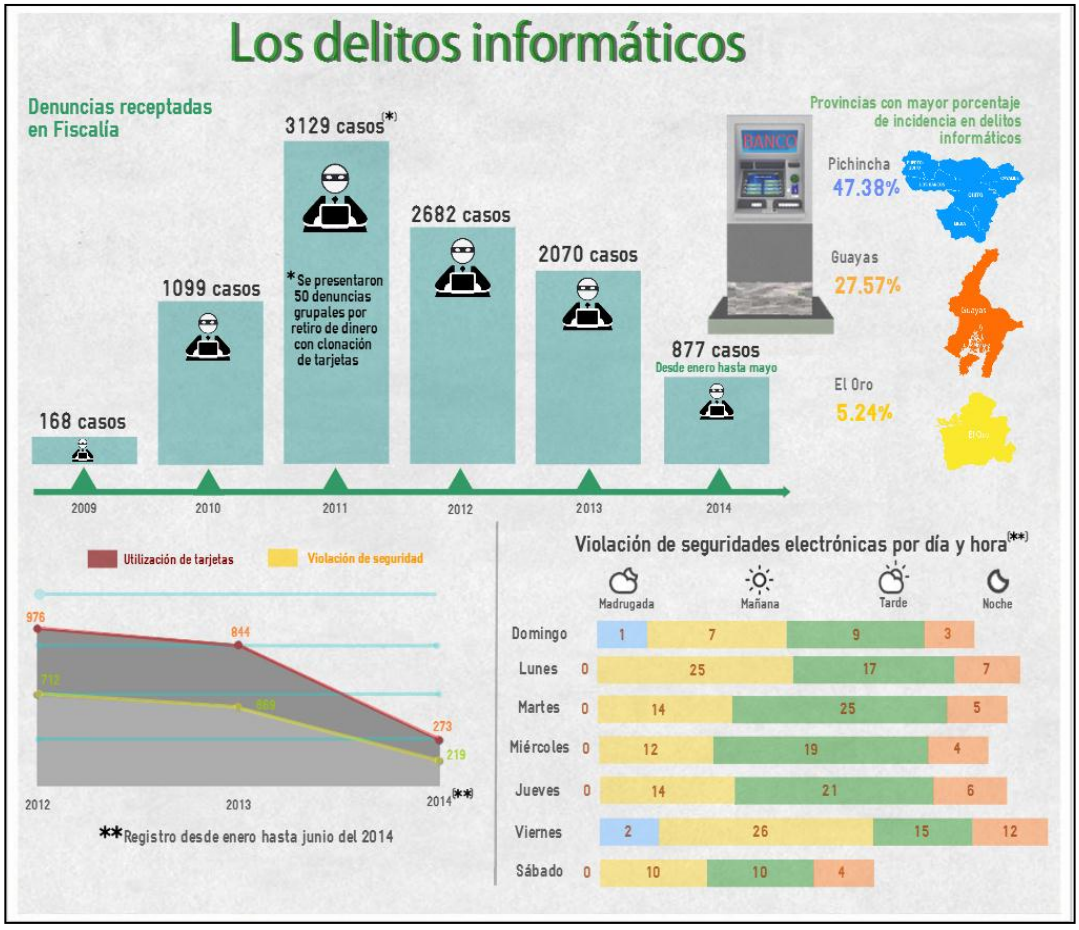


Figura 4.4: Denuncias receptadas relacionadas a delitos informáticos

Fuente: Fiscalía General del Estado.

En el Ecuador uno de los referentes en este tema, es el Phd. Enrique Mafla, quien ha intervenido en varios procesos informáticos forenses de mayor connotación en nuestro país, por citar algunos tenemos: Análisis Forense al Sistema Informático del CNE, Caso Angostura, Claves de Acceso en Municipio de Riobamba, entre otros. En varias intervenciones en medios de comunicación local, manifiesta estar de acuerdo con la tipificación de nuevos delitos de tipo informático en el actual COIP, ya que a

su criterio el país se encontraba en varios vacíos jurídicos al momento de emprender una acción legal ante el cometimiento de un delito en este contexto.

4.3 Nuevos delitos informáticos tipificados en la legislación ecuatoriana

La inclusión de los nuevos delitos informáticos que se encuentran en el actual COIP surgió de la propuesta realizada por la Policía Nacional, a través del director de la Unidad Investigación de Delitos Tecnológicos de la Policía Judicial del Ecuador, el Myr. Nicolay Zapata en agosto del 2013; dicha propuesta fue recibida y tratada en la Comisión de Justicia y Estructura del Estado perteneciente a la Asamblea Nacional.

Antes de la tipificación de los nuevos delitos no se podía sancionar a quienes usaban herramientas para capturar información, por ejemplo al usar algún tipo de sniffer, y que por su naturaleza requieren de conocimientos de sistemas, tampoco se podía sancionar a los funcionarios que en un abuso de confianza se apoderaban de claves de seguridad e información reservada, por citar un ejemplo, han existido casos en los que funcionarios se han elevado el sueldo modificando valores en los sistemas informáticos. En el caso de haber sido descubiertos, no existía el delito con el que se los podía juzgar y únicamente quedaba en una renuncia en el mejor de los casos; es decir, no existían leyes que amparen el inicio de un proceso legal de esta índole.

En su propuesta el Mayor Zapata manifestó que con estos delitos se cubren los ámbitos esenciales del convenio internacional de ciberdelincuencia del que el Ecuador no es signatario.

Los delitos que a continuación se describen son los que en Agosto del 2014 fueron tipificados e incluidos en el Actual COIP:

Tabla 4.1. Delitos Contra la Seguridad de los Activos de los S.I.

INFRACCIONES INFORMÁTICAS	**DESCRIPCIÓN**	**REPRESIÓN**
Sección Tercera: Delitos contra la seguridad de los activos de los sistemas de información y comunicación		

Revelación Ilegal de Base de Datos - COIP (Art. 229)	La persona que, en provecho propio revele información registrada, contenida en archivos, bases de datos o semejantes, a través de un sistema electrónico o informático materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas.	1 - 3 años
Interceptación ilegal de datos - COIP (Art. 230)	La persona que sin orden judicial previa, en provecho propio, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, con la finalidad de obtener información registrada o disponible.	3 - 5 años
Transferencia Electrónica de Activo Patrimonial - COIP (Art. 231)	La persona que, con ánimo de lucro, altere o modifique el funcionamiento de programa o sistema informático, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o un tercero.	3 - 5 años
Ataque a la Integridad de Sistemas Informáticos - COIP (Art. 232)	La persona que destruya, dañe, borre, deteriore, altere o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen.	3 - 5 años
Delitos Contra la Información Pública Reservada Legalmente - COIP (Art. 233)	La persona que destruya o inutilice información clasificada de conformidad con la Ley; Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años.	5 - 7 años 7 - 10 años
Acceso no consentido a un Sistema informático, telemático o de telecomunicaciones - (Art. 234)	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho.	3 - 5 años

Fuente: Código Orgánico Integral Penal - 2014

Es importante señalar que la pena por el cometimiento de algunos de estos delitos varía dependiendo quien lo realice, por ejemplo: los funcionarios públicos o empleados de Instituciones financieras que cometan el delito de Revelación Ilegal de Base de Datos, para este segmento la represión será mayor, es decir de tres a cinco años.

4.4 Iniciativas Gubernamentales

4.4.1 Creación de Comando de Ciberdefensa

El Gobierno ecuatoriano está desarrollando el Comando de Ciberdefensa que empezará a funcionar a mediados del presente año, el cual diseñará las políticas de ciberseguridad para que las Fuerzas Armadas y Policía Nacional puedan ejecutarlas.

Las organizaciones delictivas, dedicadas a vulnerar sistemas informáticos para obtener réditos económicos, mediante el uso de spam, phishing o virus, los que facilitan los robos de identidad o fraudes en línea, ahora incluyen en sus atentados a organismos estatales y sectores de servicio. Esta situación motivó a las autoridades encargadas de la seguridad en el país a coordinar la creación de un nuevo centro contra incidentes de riesgos tecnológicos.

En cuanto a los riesgos contra infraestructuras, El Ecuador hasta el año 2017 estará en proceso de inaugurar 8 obras en el sector hidroeléctrico, en cuya conformación los sistemas informáticos son vitales para su funcionamiento; el Coronel Nicolay Zapata, Jefe de la Unidad de Investigación de Delitos Tecnológicos de la Policía Judicial, manifestó que "de aquello precisamente se pueden aprovechar delincuentes o terroristas para atacar los sistemas y generar caos"; similares a los casos suscitados en países como Irán y E.E.U.U. donde se comprobaron afectaciones a sistemas Scadas mediante un malware denominado Stuxnet.

Este año el presidente Rafael Correa autorizó el uso de $ 8 millones para arrancar con este proyecto. Actualmente se está adaptando la infraestructura física en donde va a funcionar el Comando de Ciberdefensa.

El Ministerio de Defensa, Fuerzas Armadas y especialistas internacionales en tecnología han venido participando de varios seminarios internacionales de Ciberdefensa. La nueva unidad estará integrada por personal civil y militar y funcionará en la Brigada Pichincha, en Machachi.

A partir del año 2007 el país entró a una automatización de todos los servicios públicos que son estratégicos para el Estado, como los sectores: educativo, energético, transporte, salud, defensa, seguridad ciudadana; por eso el nuevo organismo de seguridad se enfocará en análisis de tendencias delictivas como malwares, spam y virus para evitar que estos paralicen el funcionamiento de servicios o prevenir ataques ciberterroristas.

En este ámbito, el Comando también auspiciará acuerdos internacionales de cooperación contra el Cibercrimen, ya que los atacantes pueden estar en cualquier parte del mundo; Samuel Linares, director del centro de ciberseguridad industrial en España, en este contexto, manifestó que "todo proyecto de infraestructura u organismo estatal que maneje información sensible o datos de los ciudadanos debe estar cuidado, ya que esos ataques cibernéticos atentan contra la seguridad interna".

Figura 4.5: Escudo del Comando de Ciberdefensa - Ecuador

Fuente: Ejército Ecuatoriano

Las organizaciones industriales, como hidroeléctricas o petroleras no cuentan con las medidas de protección básicas. En Latinoamérica son pocos los países que están tomando en serio el tema, en el ciberespacio deambulan delincuentes que utilizan diferentes tácticas para vulnerar los sistemas informáticos.

Por eso, según el experto en seguridad industrial José Valiente, el amplio espectro cibernético implica que todos los sectores están en riesgo y en el caso de los Estados existen grupos terroristas u opositores que podrían incentivar ataques para desprestigiar a un gobierno. Sin embargo, dijo que todavía no hay suficientes profesionales preparados, "existe una demanda a nivel mundial de por lo menos 1 millón de expertos en ciberseguridad que no ha sido cubierta".

El Ministerio de Defensa resaltó la necesidad de generar una doctrina propia, adaptada a la realidad del país y políticas públicas en la Ciberdefensa, por lo que el Ecuador es uno de los tres países de Sudamérica afectados por la operación "Machete", una campaña de espionaje cibernético de América Latina, y entre los espiados está el presidente Rafael Correa.

El jefe del Comando Conjunto de las FF.AA., Luis Garzón, anunció que para este año 2015 empezará a operar el Comando de operaciones de Ciberdefensa encargado de proteger a los sectores estratégicos de un posible ataque cibernético, por lo que desde ya se realiza un levantamiento de la "información crítica" del Estado en el que las Fuerzas Armadas intervendrán. Por ello, se tomará en cuenta a la Ciberdefensa como bien público.

4.4.2 Implementación de Norma INEN ISO27001 en Instituciones Públicas

La Secretaría Nacional de la Administración Pública (SNAP), con fecha 19 de septiembre del año 2013, emitió el Acuerdo Ministerial No. 166, en el cual establece como aplicación obligatoria en las entidades de la Administración Pública Central, Institucional y que dependan de la función ejecutiva, el uso obligatorio de las Normas INEN ISO/IEC 27000 para la Gestión de la Seguridad de la Información. Como anexo al acuerdo se emitió el Esquema Gubernamental de Seguridad de la

Información (EGSI), documento que está basado en la norma ISO/IEC 27002 "Código de Buenas Prácticas de Seguridad de la Información", en el que se priorizó el cumplimiento de 126 directrices.

El acuerdo manifiesta que la implementación del EGSI se realizará en cada Institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Las entidades deberán realizar una evaluación de riesgos y diseñar e implementar el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información".

Esta disposición establece fechas de cumplimiento para la ejecución de tres tareas, las cuales están representadas en la siguiente tabla:

Tabla 4.2. Fechas cumplimiento a Acuerdo 166

Descripción	**Fecha Máxima de Cumplimiento**
Conformación de Comité de Seguridad de Información, Responsable de TI y Oficial de Seguridad.	25 de Octubre del 2013
Directrices prioritarias - hitos (126)	25 de marzo del 2014
Directrices no prioritarias	25 de marzo del 2015

Fuente: Secretaría Nacional de la Administración Pública

Roberto Chávez, gerente de Riesgos en la firma auditora Deloitte Ecuador, manifestó que: "Esta norma responde a un tema que está alzando vuelo en el país, y es la seguridad en la información. Muchas personas, normalmente, creen que al hablar de seguridad informática estamos hablando de Tecnología, pero el tema va mucho más allá y abarca procesos y personas", Chávez, quien además indicó que el objetivo fundamental del acuerdo 166 es implementar un esquema gubernamental de seguridad de la información que tiene la misma idea de un sistema de gestión.

La disposición establece que el Comité de Gestión de Seguridad de la Información en las Instituciones estará conformado por el Director Administrativo, los responsables

de las áreas de Talento Humano, Tecnologías de la Información, Auditoría Interna, Legal y el Oficial de Seguridad de la Información

En lo que respecta al Oficial de Seguridad de la Información, la disposición establece las siguientes condiciones:

- No deberá pertenecer al área de Tecnologías de la Información.
- Reportará a la máxima autoridad de la Institución.
- Coordinará con las diferentes áreas a fin de recolectar información y dar cumplimiento a los hitos.
- Establecerá criterios de seguridad de Información.

Con el fin de controlar el cumplimiento a las acciones definidas en el Acuerdo 166, la Secretaría Nacional de Administración Pública realizó el año pasado un estudio de las Instituciones con el fin de verificar el cumplimiento de las acciones que logren ejecutar las 126 directrices o hitos establecidas hasta el 25 de marzo del 2014, obteniendo los siguientes resultados:

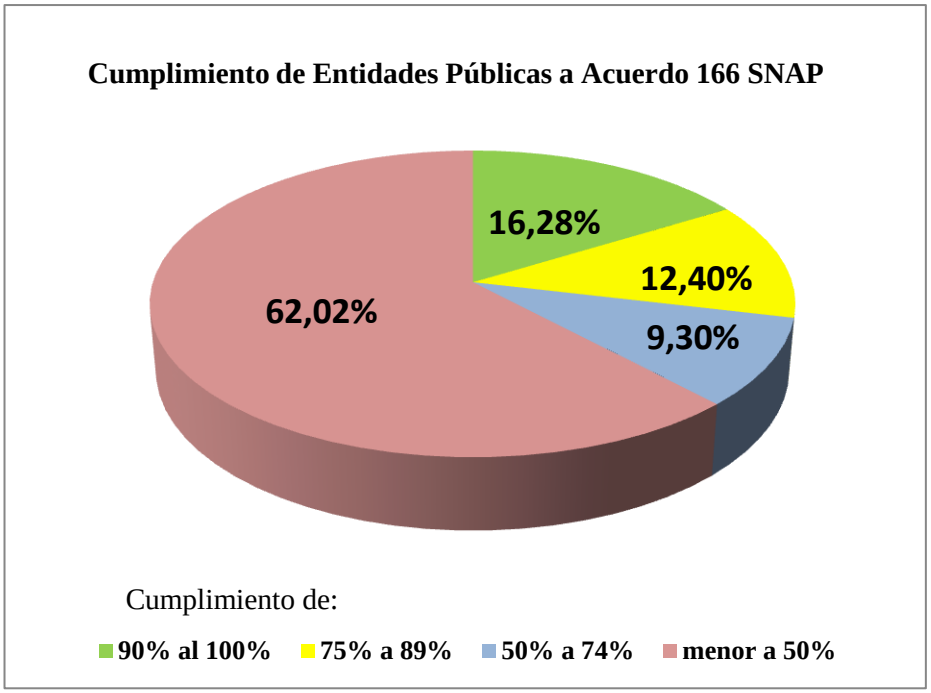


Figura 4.6: Estudio de cumplimiento de Acuerdo 166 a Instituciones Públicas

Fuente: Secretaría Nacional de Administración Pública

De 129 instituciones analizadas, sólo 21 cumplen por encima del 90%, 16 entidades tienen un nivel de cumplimiento medio al cumplir entre un 75% a 89%, 12 Instituciones tienen un nivel de cumplimiento regular por lo que apenas cumplen entre un 50% a 745 de lo dispuesto, por último 80 entidades son las que tienen un complimiento bajo ya que han ejecutado menos del 50% de lo dispuesto en el Acuerdo 166 de la Secretaría Nacional de Administración Pública (SNAP).

Por lo otro lado, Instituciones como la Corporación Nacional de Telecomunicaciones CNT se convirtió en la primera empresa pública ecuatoriana en obtener la certificación internacional de Seguridad de la Información ISO/IEC 27001.

Es preciso señalar que Seguridad de la información no es seguridad informática, ya que esta última se enfoca sólo en el aspecto tecnológico, mientras que la primera tiene un alcance de personas, procesos y tecnología.

4.4.3 Resolución JB-2012-2148 de la Junta Bancaria

La Junta Bancaria mediante resolución No. JB-2012-2148 del 26 de abril del 2012 dispuso que las instituciones del sistema financiero implementen suficientes medidas de seguridad para mitigar el riesgo de fraude mediante el uso de información y comunicaciones.

La resolución ha reformado varios artículos contenidos en las "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. Véase en Anexo 6.

La normativa, a través de la sustitución e inclusión de varios numerales del artículo 39, dispuso que las instituciones financieras implementen dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, para evitar la clonación de tarjetas de débito o de crédito.
Además, que apliquen mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales.

De acuerdo a la resolución dispondrán de un programa o sistema de protección contra intrusos (antimalware) que proteja el software instalado en el cajero automático y que detecte oportunamente cualquier anomalía en el código, configuración o funcionalidad.

Asimismo, la entidad reguladora indicó que las instituciones deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas por medio de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información.

Además, darle mantenimiento preventivo y correctivo a los cajeros automáticos cuyas claves de acceso tipo "administrador" serán únicas y se las reemplazará periódicamente.

Adicionalmente, deben disponer de cerraduras de alta tecnología y seguridades que garanticen que el acceso es controlado al interior de los cajeros.

Cabe acotar que las disposiciones dadas en dicha resolución, están alineadas al estándar internacional PCI-DSS el cual abarca el manejo y/o administración de Cajeros automáticos, tarjetas de crédito y tarjetas de débito como procedimientos relacionados a las mejores prácticas.

4.4.3.1 Estándar PCI - DSS

Es un estándar de Seguridad de Datos para la Industria de Tarjeta de Pago. Este estándar ha sido desarrollado por un comité conformado por las compañías más importantes de tarjetas (débito y crédito), como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.

Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de

crédito y débito (Pérdida de franquicias), enfrentar auditorías rigurosas o pagos de multas. Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica.

La versión actual 3.0 de la norma, especifica 12 requisitos para el cumplimiento:

1. Instalar y mantener una configuración de firewall para proteger los datos de titulares de tarjetas.
2. No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
3. Proteger los datos de titulares de tarjetas almacenados.
4. Codifique la transmisión de los datos de titulares de tarjetas a través de redes públicas abiertas.
5. Utilice y actualice regularmente el software antivirus en todos los sistemas comúnmente afectados por el malware.
6. Desarrollar y mantener sistemas y aplicaciones seguras.
7. Restringir el acceso a los datos de titulares de tarjetas de negocios
8. Asigne una ID única a cada persona que tenga acceso a una computadora.
9. Restringir el acceso físico a los datos de titulares de tarjetas.
10. Seguimiento y monitoreo de todo el acceso a los recursos de red y datos de titulares de tarjetas.
11. Probar regularmente los sistemas y procesos de seguridad.
12. Mantener una política que contemple la seguridad de la información.

4.5 Caso Práctico

La identificación de la evidencia a revelar corresponde al último caso de pedofilia y pornografía infantil descubierto en el Ecuador, en el que se logró aprehender a la persona quien era considerado como *el mayor proveedor de pornografía infantil en América Latina* a través de las redes sociales, la captura del presunto autor de este delito ocurrió el 2 de abril del 2015.

Entre las evidencias recolectadas por la Policía Nacional en el allanamiento al domicilio del presunto autor de estos delitos, constan los siguientes dispositivos:

- 1 Computador portátil
- 1 Disco duro externo
- 2 Dispositivo de memoria USB
- 1 Cámara Digital, y
- 1 Módem Access Point

La demostración del análisis forense sobre las evidencias recopiladas procura evidenciar las bondades que ofrecen varias de las herramientas de hardware y software comúnmente utilizadas por los peritos informáticos; asimismo, se aplica la norma ISO/IEC 27037 como marco de referencia en la aplicación de esta etapa.

Para la ejecución del análisis de la evidencia digital, se utilizan las siguientes herramientas forenses de software:

- Encase Forensic
- FTK Imager
- Index Analizer
- MD5-SHA1 Utility
- Entre otras.

Con el objetivo de demostrar la obtención de contraseñas activas en un equipo encendido, se utiliza la herramienta FTK Imager, mediante una captura a nivel lógico de los datos almacenados en la memoria RAM de dicho equipo.

Para la recopilación de información detallada en cuanto a la navegación web que ha realizado el presunto autor de los delitos previamente mencionados, se hace uso de la herramienta Index Analizer.

Dentro del ámbito forense informático, resultan de gran utilidad los denominados algoritmos hash, los cuales serán aplicados por cada uno de los archivos analizados

pertenecientes a los dispositivos de almacenamiento USB incautados, para lo cual se utiliza la herramienta MD5-SHA1 Utility.

Mientras que para la obtención de una fiel copia (imagen bit a bit) del disco duro externo incautado, se hace uso de un adaptador para unidades de almacenamiento (enclosure) como herramienta de hardware forense, el cual consta con terminales IDE, ATA, SATA y USB.

Adicionalmente, se incluye la demostración del uso de la esteganografía como técnica anti-forense con el objetivo de ocultar información sensible por personas que pretenden no dejar evidencias de actos ilícitos.

Finalmente, con el objetivo de evidenciar los resultados obtenidos de los análisis efectuados, se procede a utilizar el módulo de reportes y presentación de informes de la herramienta forense de software Encase Forensic, la misma que es avalada por tribunales de justicia internacionales.

.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

En los últimos años en el Ecuador se ha empezado a hablar de Informática Forense, aún falta camino por recorrer, sobre todo si se compara con otros países de la región en donde se han creado leyes específicas de delitos informáticos como tal y donde ya se habla incluso de la profesionalización de esta rama.

En la práctica de la Informática Forense a diferencia de otras disciplinas forenses, radica en que las metodologías y herramientas varían exponencialmente con el tiempo, la evolución tanto del hardware como del software es sorprendentemente acelerada, así como los mecanismos que usan los delincuentes. Para quien decida incursionar en esta carrera es de real importancia destacar el valor de estar dispuesto para el cambio.

Otra de las prioridades del perito informático es que debe familiarizarse con las herramientas cada vez que sea posible antes de que la investigación lo requiera, con esto gana tiempo valioso para la investigación.

El Ecuador al incluir en su legislación nuevos delitos de índole informático está reduciendo la brecha para que este tipo de delitos queden sin sanción alguna, como sucedía en años anteriores por la falta de tipificación de los mismos.

La informática forense ha adquirido importancia debido a que logra encontrar las evidencias requeridas y suficientes de un delito, la cual puede ser de gran valor para la resolución de un litigio llevado a los tribunales judiciales.

Este proyecto de tesis procura difundir la importancia de la Informática Forense, ya que esta ciencia integra otros conceptos como: auditoría, ingeniería inversa,

esteganografía, entre otras. De igual manera aspectos jurídicos que se enmarcan en el perfil profesional.

Este trabajo desde un inicio pretendió ser un apoyo y guía para quienes en un futuro desarrollen actividades sobre la Informática Forense en un determinado siniestro informático.

5.2 RECOMENDACIONES

Constituir y alinear una política integral de lucha en contra de la actividad ilícita para mitigar la consecución de delitos informáticos.

Ejecutar procedimientos de considerable rigurosidad en los procesos de selección de peritos informáticos, en la que éstos acrediten a más de sus conocimientos técnicos, procedimientos en manejo de evidencias e incluso avalar sus conocimientos con certificaciones tratadas en el Capítulo 3.

Introducir por parte de los organismos de control en la educación superior (SENESCYT, CEAACES, CES) la oferta académica de al menos una asignatura relacionada con la Informática Forense y/o derecho informático en las universidades del país.

Construir el primer laboratorio de análisis forense informático, tal cual ya se encuentra creado el primer laboratorio destinado a investigaciones de criminalística, este laboratorio deberá estar equipado con la más reciente tecnología para la investigación de este tipo de delitos, tanto en hardware como en software.

Ejecutar actividades relacionadas a la capacitación y/o actualización de temas concernientes a actividades ilícitas de tipo informático para interventores en varias instancias jurídicas como lo son: abogados, fiscales, jueces, entre otros..

Difundir por parte de las Universidades del país y demás centros de formación, seminarios y ofertar retos forenses que estimulen aún más a los estudiantes y futuros profesionales.

Impulsar la elaboración de programas que impliquen la difusión del peritaje informático, la legislación actual que involucra a la informática; inclusive la conformación de debates cuyo objetivo sea identificar posibles vacíos legales a pesar del ingreso de nuevos delitos en el Código Orgánico Integral Penal.

Transferencia de conocimiento en cuanto a tecnología con países de la región, o con los que se han establecido convenios internacionales, que lleven a cabo el seguimiento de los delitos informáticos.

Suscribir Convenios o tratados orientados a la cooperación internacional en este ámbito, tal cual lo vienen realizando los principales países europeos con el Convenio de Ciberdelincuencia de Budapest.

Incluir proyectos de ley por parte de los asambleístas, respecto a este tema en sus debates. Estamos en la era tecnológica donde prácticamente todos nuestros aspectos de la vida los manejamos a través de un computador, nuestro dinero en el banco, nuestro trabajo, nuestra salud, nuestro estilo de vida está prácticamente basado en la tecnología, es por eso que no podemos dejar de lado el ámbito legal del mismo.

BIBLIOGRAFÍA

Garrido, J. (2014) *Análisis Forense Digital en Entornos Windows*. España: Ediciones Oxwords.

Lima, M. L. (1994) *Delitos Electrónicos*. Porrua.

Téllez, J. (1994). *Derecho Informático*.México: Universidad Nacional Autónoma de México. Mc Graw Hill.

Convenio de Ciberdelincuencia del Consejo de Europa, (2007). *The Convention on Cybercrime*. Budapest, capital territorial de Hungría.

Herzog, A.; Shahmehri, N. y Duma, C. (2007) *An Ontology of Information Security.* Suecia: International Journal of information Security.

Informe Anual de Seguridad de Cisco (2015) disponible en URL: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html [consulta 10 de Marzo de 2015]

Casey, E. (2004) *Digital Evidence and Computer Crime*. Estados Unidos de América: Elsevier.

Cano, J. (2006) *Introducción a la Informática Forense*. Colombia: Alfaomega

Ureta, L. (2009) *Retos a Superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador*, Trabajo de Grado presentado como requisito parcial para optar al título de Magíster en Sistemas de Información Gerencial. Escuela Politécnica del Litoral. Guayaquil, Ecuador.

F.B.I. (2001) *Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence.* Virginia (Estados Unidos).

López, M. (2007) *Análisis Forense Digital (2da edición).* España: Red Iris.

Watson, D. (2013). *Digital Forensics Processing and Procedures*. Estados Unidos de América: Elsevier.

Norma ISO 27037:2012. (2012) International Standards Organization, disponible en URL: http://peritoit.com/2012/10/23/isoiec-270372012 [Consulta 12 de febrero de 2015]

Lollett, P. (2007) *Auditorìa Forense*. Venezuela: ACGAF

Tamayo, A. (2010). *Auditoría de Sistemas una Visión Práctica*. Colombia: Universidad Nacional de Colombia.

Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004).

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002).

Firma Electrónica en Ecuador. (2013) Secretaría Nacional de Administración Pública, disponible en URL: http://www.administracionpublica.gob.ec/firma-electronica/ [consulta 3 de octubre de 2014]

Ley de Propiedad Intelectual. (1998).

Ley Especial de Telecomunicaciones, (2014). Disponible en URL: http://www.arcotel.gob.ec/ [consulta 5 de enero de 2015]

Ley de Control Constitucional (2009).

Estudio de Piratería Mundial de Software. (2012). Business Software Alliance, disponible en URL: http://globalstudy.bsa.org/2011/downloads/translatestudy/2011GlobalPiracyStudy_es.pdf [consulta 28 diciembre de 2013]

Transparencia es del 65% en las entidades públicas del Estado. (2012). Diario El Telégrafo, disponible en URL: www.telegrafo.com.ec/transparencia-es-del-65-en-las-entidades.html

Riofrío, J. (2004). *La Prueba Electrónica*. Colombia: TEMIS.

Del Peso, E. (2003). *Peritajes Informáticos (2da edición)*. Chile: Editorial Díaz de Santos.

Reglamento del Sistema Pericial de la Función Judicial, (2014), Consejo de la Judicatura, disponible en URL: http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2014cj/040-2014.pdf [consulta 3 enero de 2015]

Normativa de Actuación y Honorarios de Peritos de la Función Judicial, (2013), Consejo de la Judicatura, disponible en URL: http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2013cj/052-2013.PDF [consulta 6 de enero de 2015]

Código Orgánico Integral Penal del Ecuador, (2014).

Panorama del Derecho Informático en América Latina, (2013), Comisión Económica para América Latina y el Caribe, disponible en URL: http://www.cepal.org/ddpe/publicaciones/xml/8/38898/w302.pdf [consulta 8 de agosto de 2014]

Uso de internet en el Ecuador por área. (2013), Instituto Nacional de Estadísticas y Censos, disponible en URL: http://www.ecuadorencifras.gob.ec/documentos/webInec/Estadisticas_Sociales/TIC/Resultados_principales_140515.Tic.pdf [consulta 5 diciembre de 2014]

Acurio, S. (2011), *Perfil Sobre los Delitos Informáticos en el Ecuador*. Recuperado de http://app.ute.edu.ec/content/3254-42-10-1-6-7/Perfil%20de%20los%20Delitos%20Informaricos%20%20Ecuador%20-%20Fiscalia.pdf

Ciberseguridad, Escenarios y Recomendaciones. *Revista Nuestra Seguridad, (Edición 17), Pág. 10 - 11*. Ecuador.

Creación de Comando de Ciberdefensa. (13 de Septiembre de 2014). *Diario El Ciudadano.* Recuperado de http://www.elciudadano.gob.ec/la-ciberdefensa-es-una-necesidad-en-los-tiempos-actuales

Acuerdo 166. (2013), Secretaría Nacional de Administración Pública, disponible en URL: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2013/11/Acuerdo-No.-1661.pdf

Resolución JB-2012-2148. (2012), Superintendencia de Bancos, recuperado de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

Estándar *PCI-DSS*. (2014), Recuperado de https://es.pcisecuritystandards.org/

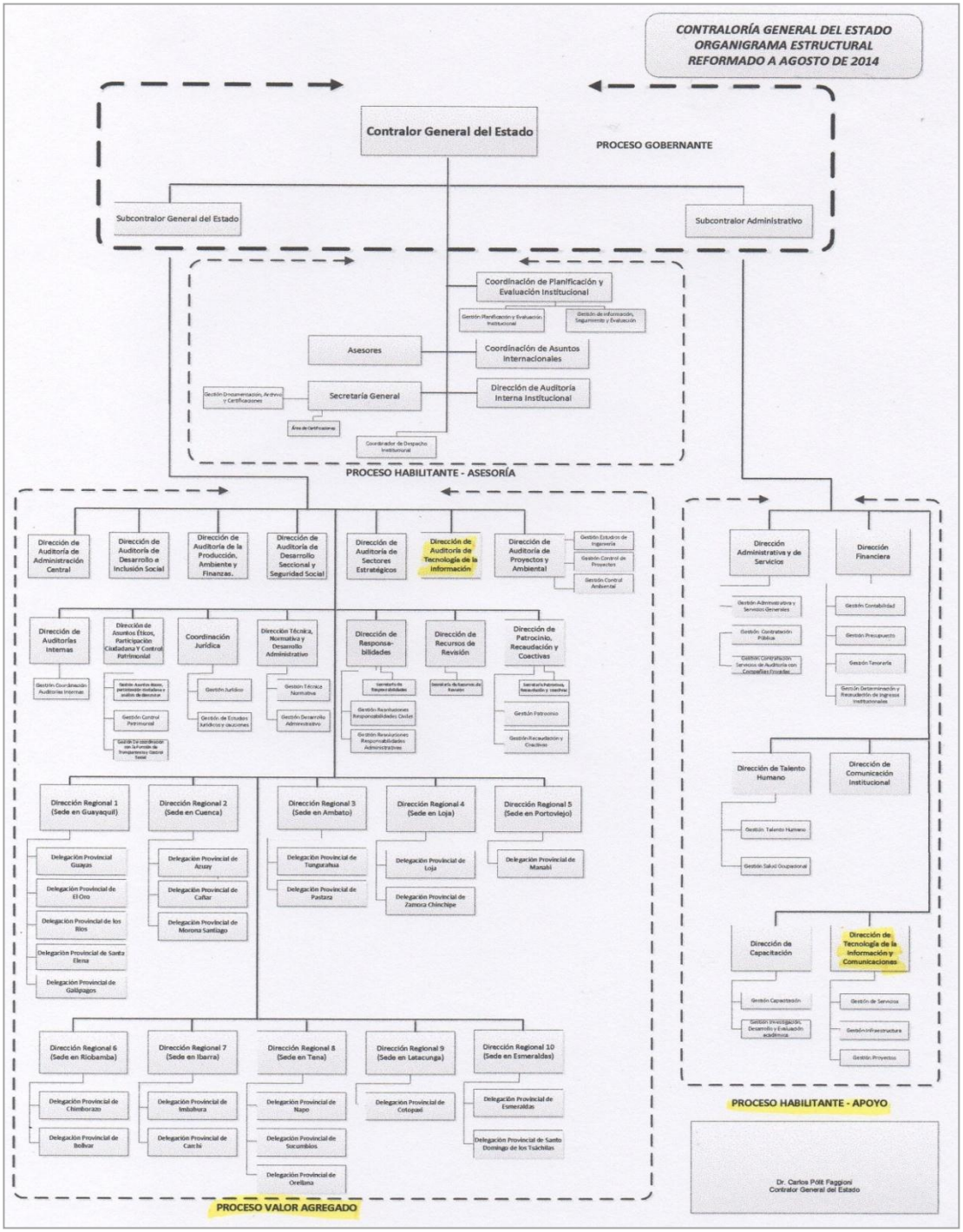
Caso de Pornografía Infantil en el Ecuador (2015), Ecuavisa, disponible en URL: http://www.ecuavisa.com/articulo/noticias/nacional/104580-detienen-quito-al-mayor-proveedor-pornografia-america-latina [consulta 3 abril de 2015]

Astudillo, K. (2013), *Hacking Ético 101*. Ecuador.

ANEXOS

Anexo 1

Organigrama de la Contraloría General del Estado.



Fuente: Contraloría General del Estado

Anexo 2

Sub-Especialidades reconocidas por el Consejo de la Judicatura.

Sub-Especialidades reconocidas en el Consejo de la Judicatura	
Accidentes de tránsito/análisis vial	Ingeniería ambiental
Acuacultura	Ingeniería civil
Administración de empresas	Ingeniería comercial
Análisis sustancias estupefacientes, drogas y afines	Ingeniería eléctrica - Electrónica
Arquitectura	Tributación fiscal
Asuntos aduaneros, clasificación, valoración	Ingeniería forestal
Audio, video y afines	Ingeniería genética
Auditoría	Ingeniería petrolera e hidrocarburos
Avaluador de bienes inmuebles	Ingeniería química
Avaluador de bienes muebles	Ingeniería geología - minas
Avalúo de tránsito	Ingeniería agrícola/agroindustrial
Avalúo inmuebles	Inspección ocular técnica (OIT)
Avalúo muebles	Joyería
Balística	Jurisprudencia
Bancario, fiduciario, bursátil	Liquidador
Biología	Liquidador de costas
Bioquímica farmacéutica	Liquidador laboral
Catastros	Mecánica automotriz
Ciencias biológicas/biología	Medicina de emergencia
Cirugía general y especializada	Medicina general
Clínico	Medicina laboral - Legal
Contabilidad, finanzas	Impacto ambiental
Contador público	Naval
Criminalística	Odontología forense
Dactiloscopía	Odontología/odontología forense
Derecho	Orientación familiar
Documentología	Portugués
Economía general	Psicología
Educación en bachillerato	Psicología clínica
Educación en general	Psicología criminal
Educación inicial	Psicología educativa
Explosivos	Psicología infantil
Finanzas	Psiquiatra
Forense/legal	Quichua/kichwa
Genética	Química/ farmacéutica
Ginecología	Topografía
Grafología	Química forense
Identidad humana	Radiología y imagenología
Informática y telecomunicaciones	Reconstrucción virtual
Ingeniería finanzas	Revenidos químicos
Ingeniería industrial	Ingeniería mecánica
Ingeniería informática o de sistemas	Seguridad industrial

Fuente: Consejo Nacional de la Judicatura

Anexo 3

Respuesta a Solicitud de Información al Concejo de la Judicatura.

CONSEJO DE LA JUDICATURA

Guayaquil, 12 de enero del 2015
Oficio Nº 09-CSP-CJ-VSR-SCO-2015

Sr.
RÓMULO GABRIEL VERDEZOTO ACUÑA
Ciudad.-

De mi consideración:

En atención a su escrito S/N, ingresado en vuestra institución el 8 enero del 2015 a las 11h53; mediante el cual solicita se proporcione información sobre **el Número de Peritos acreditados a nivel Nacional por Provincia en las diferentes ramas actualizados a la fecha actual**, referente a su tesis "El rol de Auditoria Forense ante los nuevos delitos informáticos tipificados en el actual Código Orgánico Integral Penal del Ecuador".

Por medio de la presente cumplo en informar el número actualizado de Peritos acreditados por el Consejo de la Judicatura del Guayas en las especialidades de Informática y Telecomunicación e Ingeniería de Informática y de Sistema.

ESPECIALIDAD	NUMERO DE PERITOS ACREDITADOS
INFORMATICA Y TELECOMUNICACIÓN	2
INGENIERÍA DE INFORMATICA Y DE SISTEMA	9
TOTAL	**11**

Particular que comunico para su conocimiento y fines pertinentes.

Atentamente,

Ab. Verónica Sánchez Rendón
Coordinadora del Sistema Pericial
Dirección Provincial del Guayas
Consejo de la Judicatura

Elaborado por: Silvia Cassanello	File:

Anexo 1

DIRECCIÓN PROVINCIAL - GUAYAS
Pedro Moncayo 934 entre 9 de Octubre y Vélez. Guayaquil
(04) 2 599 600
www.funcionjudicial.gob.ec

Hacemos de la justicia una práctica diaria

e100d1e1-9aab-11e4-8000-080037d23282

Fuente: Los autores

Anexo 4

Formato de Informe Pericial provisto por el Consejo de la Judicatura

CONSEJO DE LA JUDICATURA

FORMATO DE INFORME PERICIAL

Las peritas y peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO QUE REGULA EL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL. Por lo tanto, el **presente formato es de uso obligatorio para la presentación de los informes periciales**, sin perjuicio de lo establecido en normas legales específicas.

"INFORME PERICIAL

1. **DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA**

TRIBUNAL/JUZGADO/FISCALÍA	
No. de Proceso/No. de Indagación Previa o Instrucción Fiscal	
Nombre y Apellido del Perito/a	
Profesión, Oficio, Arte, o Actividad calificada	
No. de Calificación y Acreditación	
Fecha de terminación de la calificación y acreditación	
Dirección de contacto	
Teléfono fijo de contacto	
Teléfono celular de contacto	
Correo electrónico de contacto	

2. **PARTE DE ANTECEDENTES**, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

3. **PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE**, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. El perito/a deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

4. **PARTE DE CONCLUSIONES**, luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe

técnico. El informe solamente versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá sobre el accionar de las partes procesales en el caso en particular. Las conclusiones solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver, y será tomado en consideración para la evaluación del perito/a.

5. **PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO,** deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc.); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas del perito/a para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos, o con la explicación técnica y científica exigida en este numeral. El perito/a deberá razonar y motivar diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, será considerado al momento de la evaluación del perito.

6. **OTROS REQUISITOS.** si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, la perita y el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

7. **INFORMACIÓN ADICIONAL,** el perito o la perita podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; y, siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

8. **DECLARACIÓN JURAMENTADA,** el perito o la perita deberá en la parte final del informe, declarar bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como también, que toda la información que ha proporcionado es verdadera.

9. **FIRMA Y RÚBRICA,** al final del informe se deberá hacer constar la firma y rúbrica del perito o perita, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."

Fuente: http://www.funcionjudicial.gob.ec/

Anexo 5

Tabla de Honorarios de Peritos según Especialidad.

AREA Y ESPECIALIZACION	ACTIVIDAD	HONORARIOS
ADUANA: Asuntos aduaneros, clasificación, valoración.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.
ADMINISTRACION: Administración de empresas, finanzas, síndico de quiebras, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
ALIMENTACION: Arte culinario, alimentación de alimentos y bebidas, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cinco (5) veces la RBU, según la materia y complejidad del análisis.
ARQUEOLOGIA: Arqueología, numismática, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.
ARQUITECTURA, INGENIERÍA CIVIL: Arquitectura, diseño interior, diseño gráfico, diseño de productos, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
CIENCIAS BIOLÓGICAS: Ciencias biológicas/biología, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.
BELLAS ARTES: Artes plásticas, escultor, escritor, gemólogo, joyería, museólogo, músico/producción musical, pintor, teatro, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.

COMUNICACION: Comunicación, animación digital, artes audiovisuales y multimedia, cine y vídeo, comunicación publicitaria, comunicación visual, interactividad y multimedia, periodismo/periodismo.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.
CONTABILIDAD Y AUDITORIA: Auditoría, contador público, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
CONTABILIDAD Y AUDITORIA: Liquidador, liquidador de costas, liquidador laboral.	Informe pericial.	Treinta por ciento (30%) de la RBU.
CRIMINALISTICA: Accidentes de tránsito/análisis vial, avalúo de tránsito, análisis de sustancias estupefacientes, drogas y afines, balística, criminología, dactiloscopia,	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.
CRIMINALISTICA: Acústica, audio, vídeo y afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.
DERECHO: Derecho, contratación pública, propiedad intelectual, marcas y patentes, antropología jurídica, derecho tributario, derecho internacional privado, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
ECONOMIA: Bancario, fiduciario, bursátil, contabilidad, finanzas, análisis financiero, economía general, tributación fiscal.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia.
FILATELIA: Filatelia, paleografía (documentos antiguos), otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.

FOTOGRAFIA: Fotografía, fotografía digital, fotografía publicitaria, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.
HOTELERIA Y TURISMO: Hotelería y turismo, gestión hotelera, ecoturismo/gestión ambiental, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cinco (5) veces la RBU, según la materia y complejidad del análisis.
INGENIERIA: Aeronáutica, acuicultura, en procesos biotecnológicos, electromecánica, eléctrica, electrónica, ingeniería en finanzas, genética, ingeniería informática o de sistemas,	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
TRADUCTORES DE IDIOMAS Y LENGUAS ANCESTRALES:	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde 0,05% a 0,10% de la RBU por cada palabra traducida.
TRADUCTORES DE IDIOMAS:	Participación en diligencias y/o audiencias.	10% de la RBU por cada hora, de asistencia a la diligencia y/o audiencia.
TRADUCTORES DE LENGUAS ANCESTRALES, Intérprete de señas, intérprete de braille, otras actividades afines.	Participación en diligencias y/o audiencias.	10% de la RBU por cada hora, de asistencia a la diligencia y/o audiencia, El pago será proporcional por la fracción de hora de asistencia.
PEDAGOCIA Y EDUCACION: Educación en general, educación inicial, educación básica, educación en bachillerato, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.
QUIMICA: Biología molecular, explosivos, química en alimentos, química forense, especialidades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta tres (3) veces la RBU, según la materia y complejidad del análisis.

SALUD HUMANA: Enfermería, orientación familiar, terapia física/rehabilitación física, obstetricia, optometría, quiropráctico, nutrición humana, especialidades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cuatro (4) veces la RBU, según la materia y complejidad del análisis.
TRABAJO SOCIAL: Trabajo social/gestión social, otras actividades afines.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cinco (5) veces la RBU, según la materia y complejidad del análisis.
OTRAS ACTIVIDADES TECNICAS Y/O CIENTIFICAS ESPECIALIZADAS DE INDOLE PROFESIONAL.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.
Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta cinco (5) veces la RBU, según la materia y complejidad del análisis.	OTRAS ACTIVIDADES ESPECIALIZADAS DE INDOLE NO PROFESIONAL.
MEDICINA HUMANA: cardiología, cirugía general y especializada, clínico, dermatología, diabetología, ecografía, ecografista, forense/legal, neumología, gastroenterología, genética, geriatría, ginecología, hematología, y medicina natural en general, infectología, mastología, medicina interna, medicina laboral, medicina nuclear, nefrología, neurocirugía, neurología, odontología odontología forense.	Examen pericial, informe, actividades del artículo 26 de este reglamento.	Desde el 50% de RBU hasta diez (10) veces la RBU, según la materia y complejidad del análisis.

Fuente: Reglamento del Sistema Pericial Integral de la Función Judicial.

Anexo 6

Resolución JB-2012-2148

RESUELVE:

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:

ARTÍCULO 1.- En el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del título II "De la organización de las instituciones del sistema financiero privado", efectuar las siguientes reformas:

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 (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 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 o 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 renumerar 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 reemplazadas 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. Incluir como tercera disposición transitoria, la siguiente:

"**TERCERA.-** Las instituciones financieras informarán a la Superintendencia de Bancos y Seguros, en el plazo de treinta (30) días, a partir de la publicación en el Registro Oficial de la presente reforma, sobre el nivel de cumplimiento de las disposiciones de seguridades mencionada en el artículo 39, de este capítulo.

El Superintendente de Bancos y Seguros determinará, de ser el caso, los cronogramas de adecuación, para la implementación de las medidas de seguridad señaladas en el citado artículo, cuyo plazo no excederá de nueve (9) meses, debiendo remitir trimestralmente un informe de avance de la implementación."

ARTÍCULO 2.- En el capítulo V "De la gestión del riesgo operativo", del título X "De la gestión integral y control de riesgos", efectuar las siguientes reformas:

1. En el artículo 2, efectuar los siguientes cambios:

1.1 En el numeral 2.12, sustituir la frase "... y toma de decisiones" por "... , toma de decisiones, ejecución de una transacción o entrega de un servicio;"

1.2 En el numeral 2.34, eliminar la letra "... , y ...", incluir los siguientes numerales y renumerar el restante:

"**2.35 Calidad de la información.-** Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella;

2.36 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente;

2.37 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones;

2.38 Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda;

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";

4.3.10 Puntos de venta (POS y PIN Pad).- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente:

4.3.10.1 Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización;

4.3.10.2 A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura; y,

4.3.10.3 Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip;

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

Fuente: Superintendencia de Bancos y Seguros del Ecuador