ISSN 0798 1015

REVISTA ESPACIOS

HOME | Revista ESPACIOS | ÍNDICES / Index | A LOS AUTORES / To the AUTHORS

Vol. 39 (Nº 42) Año 2018 • Pág. 15

Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad

Application of forensic science in cybercrime in Ecuador and its punishability

Carlos ALCÍVAR Trejo 1; Glenda BLANC Pihuave 2; Juan CALDERÓN Cisneros 3

Recibido: 19/04/2018 • Aprobado: 04/06/2018

Contenido

RESUMEN:
El presente artículo se abordará un análisis comparativo sobre varios delitos informáticos en algunos países vs el Ecuador, y como estos han evolucionado con la normativa punible, uno de los mayores retos del presente siglo es lograr un buen nivel de seguridad en el ciberespacio. El incremento cuantitativo y cualitativo del uso de las TIC en todas las actividades sociales, educativas, mercantiles, de publicidad y demás, han dejado de ser instrumentos opcionales en la vida cotidiana.
Palabras-Clave: Delitos Informáticos, Cibercrimen, Legislación, Análisis Forense.

ABSTRACT:
This article will address a comparative analysis of several cybercrimes in some countries vs. Ecuador, and as these have evolved with punishable regulations, one of the greatest challenges of this century is to achieve a good level of security in cyberspace. The quantitative and qualitative increase in the use of ICT in all social, educational, commercial, advertising and other activities have ceased to be optional instruments in everyday life.
Keywords: Computer Crimes, Cybercrime, Legislation, Forensic Analysis.

1. Introducción

La ciberdelincuencia o Cybercrimen engloba cualquier acto criminal que trata con las computadoras y redes (llamado hacking). Además, el crimen cibernético también incluye los delitos tradicionales realizados a través de Internet. Por ejemplo; los crímenes de odio, el telemarketing, el fraude en Internet, el robo de identidad, y robo de la cuenta de tarjeta de crédito son considerados como delitos cibernéticos cuando las actividades ilegales se cometen mediante el uso de una computadora y el Internet.

Un delito es definido como "una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria al Derecho), culpable y punible. Supone una conducta infraccional e

intencional del derecho penal, es decir, una acción u omisión tipificada y penada por la ley" (COIP, 2014, p. 20).

La conducta que es un acto humano que como persona natural o jurídica se describe como infracción penal, siendo sus modalidades: la acción que es el hacer; y, la omisión que es el "no hacer" que genera consecuencias jurídicas.

La tipicidad es la adecuación de la conducta a los elementos del tipo; es decir, a la descripción de una conducta vinculada con una pena. De tal suerte, que tipicidad no es lo mismo que tipo penal, siendo la tipicidad entendida como la subsunción de la conducta al tipo; mientras que, el tipo penal es el precepto que se describe hipotéticamente como infracción.

La antijuricidad o antijuridicidad que se considera como la lesión o lesividad es lo contrario a derecho, que puede ser formal y material; en el sentido formal, es la relación de contradicción de la conducta y todo el ordenamiento jurídico. En el sentido material, es la afectación o puesta en peligro de un bien jurídico.

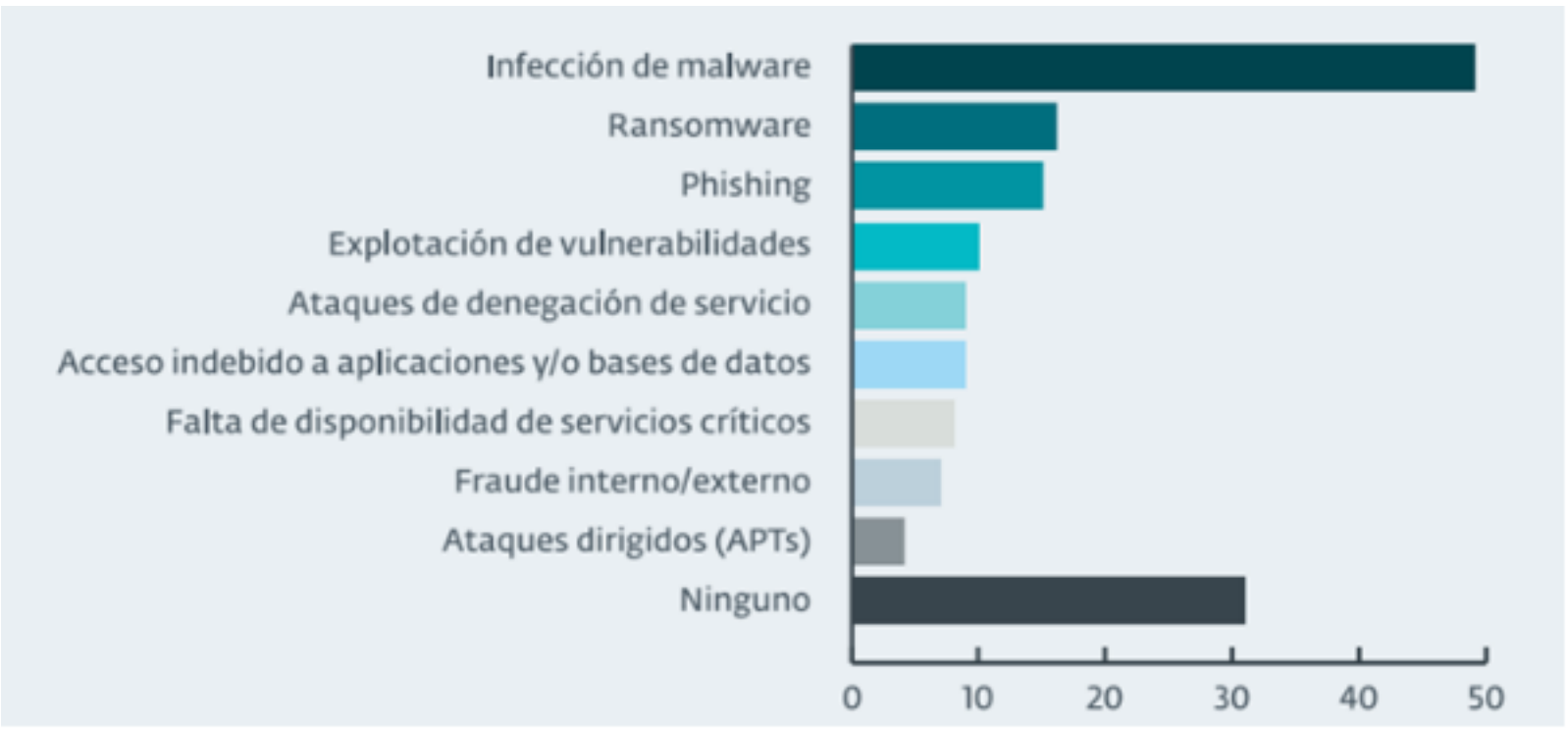
1.1. Seguridad en Internet

Los usuarios cibernéticos necesitan conocer que a través de Internet estamos expuestos a diversas formas de delinquir, tanto a la diversificación de los delitos tradicionales como a nuevos actos ilícitos como son los delitos informáticos y los delitos computacionales.

Los delitos Informáticos son aquellos en los que nuestros ordenadores, dispositivos móviles, redes de Internet son atacados por vías informáticas, logrando que el software de nuestro equipo se dañe o que la red o servidores queden inhabilitados, con el fin de violar, e introducirse en un sistema operativo para obtener información de dichoso porte magnético para usarlo en favor suya o de terceros ajenos a la empresa.

Estos actos pueden llevarse a cabo de forma rápida y sencilla, en ocasiones se cometen en cuestión de segundos, utilizando solo un equipo informático y sin estar presente físicamente en el lugar de los hechos, lo que complica demostrar las respectivas pruebas.

Figura 1
Incidentes de seguridad en empresas de Latinoamérica



Fuente: *https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf*

2. Metodología

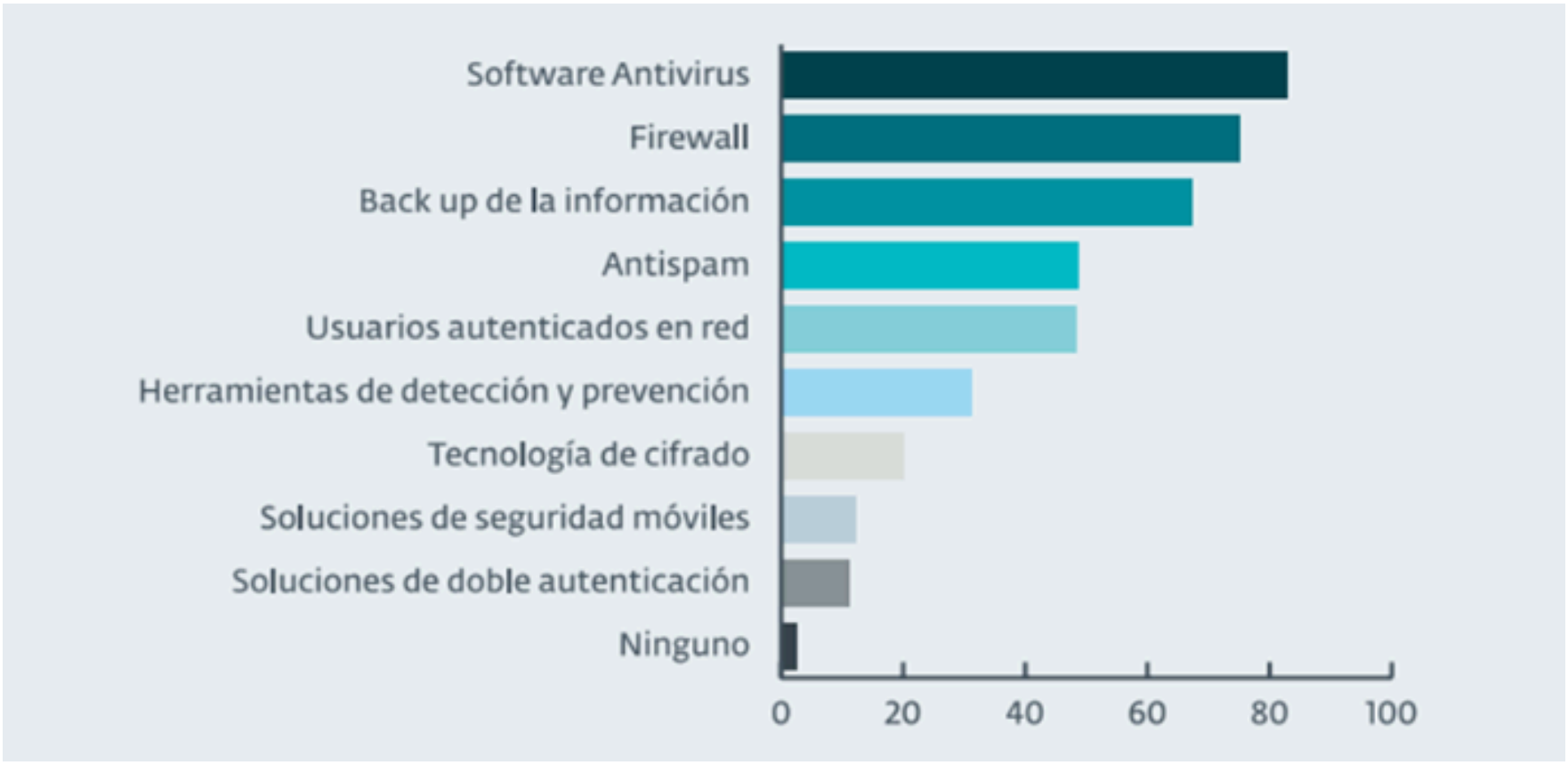
Se utilizaron fuentes de información primaria y secundaria, obtenidos de la base de datos del WOS y Google Académico, sobre la información de las TIC, los delitos computacionales, que utilizan medios informáticos como por ejemplo la utilización de una computadora

conectada a una red bancaria, para cometer delitos tradicionales como una estafa, robo, o hurto, también se considera como delito computacional a la violación de email. (Calderón, 2010), que genera información sobre equipamiento, acceso y uso del computador, internet y celular, en el hogar, proporcionando insumos para el análisis, las consecuencias de la sociedad del conocimiento sean estos buenos o malos. Se presenta también como en el Ecuador(Lazzeri, Urbina, Leonardo, & Morales, 2017), se beneficia de los avances y de los cambios tecnológicos, para enfrentar los dilemas relacionados con áreas como: inclusión social, educación, matriz productiva.

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo. (seguros informáticos, 2009).

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos. (seguros informáticos, 2009).

Figura 2
Controles de seguridad más implementados en Latinoamérica



Fuente: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

2.1. La Ciencia Forense

La palabra forense viene del adjetivo latino forensis, que significa "perteneciente o relativo al foro". En la Antigua Roma, una imputación por crimen suponía presentar el caso ante un grupo de personas notables en el foro. Tanto la persona que se la acusaba por haber cometido el crimen como el denunciante tenían que explicar su versión de los hechos. La argumentación, las pruebas y el comportamiento de cada persona determinaban el veredicto del caso. Existen muchas definiciones de ciencia forense, todas tienden a hacer referencia que es auxiliar del derecho.

Con esta definición citada, podemos citar que es la aplicación de prácticas científicas dentro del proceso legal. Esencialmente esto se traduce en investigadores altamente especializados o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios. De una forma simple, podríamos definir la informática forense como un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales.

Podríamos definir a la ciencia forense digital, como el uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop DFRWS). La extracción de una evidencia digital se realizará a partir de una utilización amplios recursos, por medio de software, hardware o herramientas para este propósito. De este modo, la extracción de una evidencia puede ser realizada a través de los más variados métodos. (Taborda, 2017).

Una de las técnicas es la Informática forense que recolecta y utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías avanzadas. Un experto en informática forense utiliza estas técnicas para descubrir evidencia de un dispositivo de almacenaje electrónico. Los datos pueden ser de cualquier clase de dispositivo electrónico como discos duros, cintas de respaldo, computadores portátiles, memorias extraíbles, archivos y correos electrónicos.

La Investigación Forense tiene las siguientes guías a nivel internacional:

- RFC 3227
- IOCE
- DoJ1 y DoJ2
- Hong Kong

Las herramientas de Software que son las más utilizadas para realizar la investigación forense digital son:

- Winhex,
- Hélix,
- Encase

Existen certificaciones profesionales para especializarse en este campo de estudio que son:

- Forense: Certified Forensic, Computer examiner (IACIS)
- Seguridad Informática: Association of Certified Fraud Examiners (CFE)

En el Ecuador el Consejo de la Judicatura (CJ), acredita a los peritos que no solo requieren de conocimientos en informática, sino también en leyes o viceversa. Deben buscar evidencias de un delito y redactar informes técnicos forenses, sin establecer responsables sin embargo existe déficit de este tipo de profesionales algunas provincias del Ecuador y según estadísticas del CJ a nivel nacional son pocos los peritos registrados.

Figura 3
Estadísticas de peritos informáticos en Ecuador

Fuente: Consejo de la Judicatura del Ecuador

3. Resultados

Según el informe de evolución del 'cybercrimen' entre 2011 y 2020 en Ecuador por Kaspersky, tendrán gran demanda en el mercado negro:

- El espionaje comercial,
- El robo de bases de datos
- Los ataques a la reputación de las empresas

Los datos personales de usuarios serán de principal interés de los cyber delincuentes. En el actual Código Orgánico Integral Penal (COIP) del Ecuador se tiene los siguientes delitos informáticos:

Cuadro 1
Delitos informáticos y su punibilidad

DELITOS	PUNIBILIDAD
Base ilegal de datos	1 a 3 años 3 a 5 años
Daño informático	3 a 5 años y 10 a 20 RMU
De la intrusión indebida a los sistemas informáticos, de información o telemáticos	3 a 5 años y 10 a 20 RMU 5 a 7 años
Falsificación electrónica	5 a 7 años
Falsedad informática	7 a 9 años
Estafa informática	9 a 11 años

Fuente: Código Orgánico Integral Penal del Ecuador

De los casos suscitados en Ecuador en cuanto a Delitos Informáticos, de enero a diciembre del 2010, se recibieron más de 866 denuncias en diferentes fiscalías del país por delitos tradicionales cometidos por y con mecanismos informáticos, de las cuales 697 fueron apropiación ilícita, 86 denuncias propiamente de delito informático como vulneración a páginas de servicio público, 82 a páginas de servicio privado y 1 por estafa utilizando medios informáticos. En Ecuador, los ciberdelitos están tipificados en el Código Orgánico Integral Penal (COIP) como una medida para perseguirlos y fijar sanciones.

De acuerdo con estadísticas del Delitoscopio de la Dirección de Política Criminal de Fiscalía del Ecuador, los delitos que se han denunciado con mayor frecuencia a escala nacional, en el 2015, son:

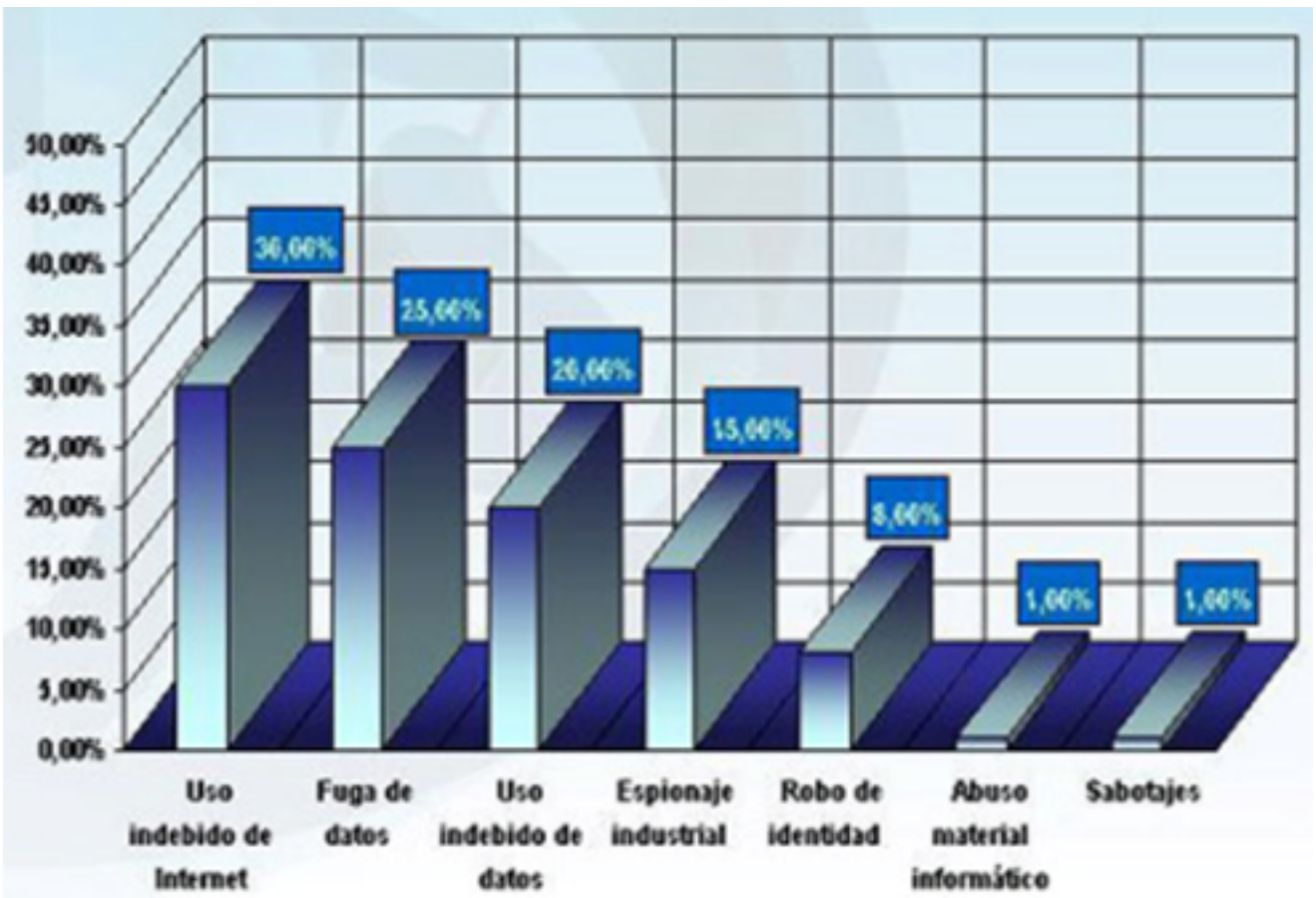
Cuadro 2
Estadísticas de delitos informáticos

Delito:	Artículo COIP:	Denuncias enero-agosto 2015
Apropiación fraudulenta por medios electrónicos	190	646
Apropiación fraudulenta por medios electrónicos con inutilización de alarmas, descifrado de claves o encriptados.	190	147
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	234	91
Ataque a la integridad de sistemas informáticos	232	45
Transferencia electrónica del activo patrimonial	231	36
Interceptación ilegal de datos	230	34
Revelación ilegal de base de datos	229	19
Transferencia electrónica del activo patrimonial. La persona que facilite o proporcione su cuenta bancaria para recibir de forma ilegítima un activo.	231	4
Ataque a la integridad de sistemas informáticos. Persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya dispositivos o programas informáticos maliciosos.	232	2
Delitos contra la información pública reservada legalmente	233	2
Total		**1026**

Fuente: Delitoscopio de la Dirección de Política Criminal de Fiscalía del Ecuador

En la Fiscalía del Ecuador creó la Unidad Especializada Contra la Ciberdelincuencia con personal debidamente capacitado en esta área, mediante la que será posible interceptar información que circula por la Internet. Según información de la Fiscalía se tiene los siguientes motivos de peritaje informático:

Figura 4
Motivos de Peritaje informático



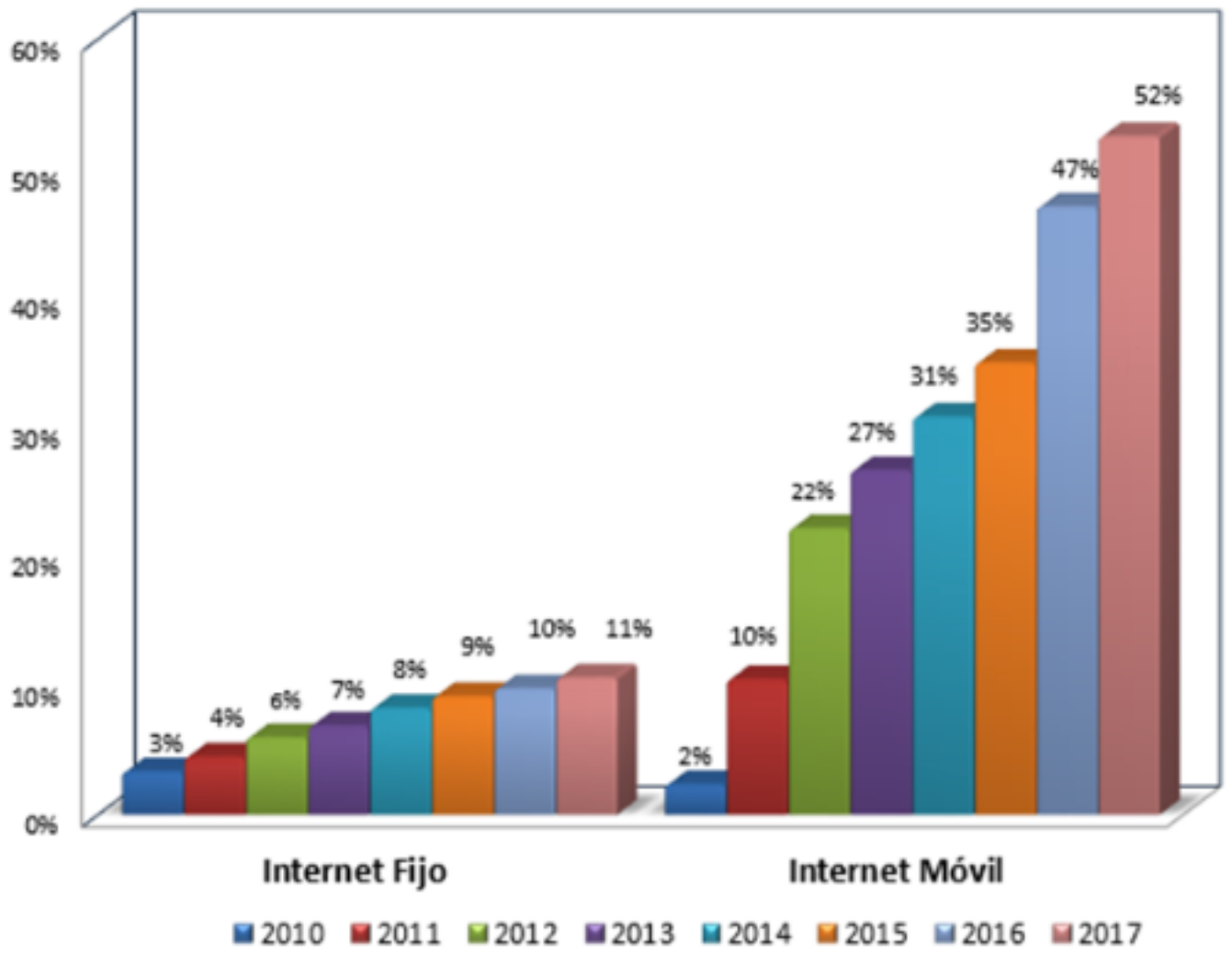
Fuente: https://www.fiscalia.gob.ec/

Otro ente que aporta con información cuando se realizan los peritajes informáticos es la Agencia de Regulación y Control de las Telecomunicaciones que es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro

radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes, además emite estadísticas del sector de las telecomunicaciones (ARCOTEL, 2018).

En el año 2017 por cada 100 habitantes en Ecuador 52 tienen internet móvil, y 11 tienen internet fijo, esto da apertura que la población ingrese al Internet y sea más vulnerable ante la cyber delincuencia, a continuación, la evolución del internet a partir del año 2010.

Figura 5
Cuentas Internet fijo y Móvil por cada 100 habitantes



Fuente: https://www.arcotel.gob.ec./servicio-acceso-internet/

Un caso es el 9 de enero de 2016, la Fiscalía de Ecuador acusó de asociación ilícita a la supuesta banda de hackers o delincuentes cibernéticos, quienes habrían manipulado los sistemas informáticos de la Secretaría de Educación Superior (Senescyt) y de la Agencia Nacional de Tránsito (ANT). Los Hackers habrían inscrito 366 títulos universitarios en la web de la Secretaría de Educación Superior, que ya fueron bajados del registro. Por cada uno, según el grado, solicitaban entre USD 1000 y USD 10000. Los más caros eran los doctorados y en la Agencia Nacional de Tránsito (ANT) también fue vulnerado el sistema informático donde se identificaron 600 licencias de conducir que fueron emitidas sin el proceso legal, por cada documento cobraban entre USD 1000 y USD 3000 (El Comercio, 2016).

---

4. Conclusiones

Los funcionarios públicos de la Fiscalía que analicen los delitos informáticos deben especializarse en investigaciones como: Procedimiento Técnico para la Investigación, Cadena de Custodia de la Evidencia Digital, Identificación de IP internacionales y presentación de los elementos de convicción en las Etapas del Proceso Penal.

Los delitos informáticos se incrementan a la par del desarrollo tecnológico, constituyéndose en un fenómeno creciente en todo el mundo.

La investigación de los ciberdelitos es compleja, debido principalmente al desconocimiento de técnicas en la investigación en los funcionarios públicos y la falta de coordinación interinstitucional del sector a cargo de las telecomunicaciones.

Programas de capacitación concientización legal-informático-legal, para el uso seguro y responsable de las tecnologías.

La conducta humana siempre ha sido compleja y en muchas ocasiones el origen de sus actos es desconocido, de allí nacen diferentes ciencias y disciplinas que buscan una respuesta al comportamiento criminal de los seres humanos.

Es fundamental en el reconocimiento, la identificación e individualización de las evidencias digitales o materiales con el fin de determinar si un hecho es delito, cómo se cometió, dónde, cuándo y quién lo cometió.

Referencias bibliográficas

Abogados Ec (s.f.). Memorias III Foro Seguridad Digital 2016. Obtenido de http://www.abogados.ec/2016/10/12/memorias-iii-foro-seguridad-digital-2016/

Asamblea Nacional, (10 de febrero de 2014). Código Integral Penal. Registro Oficial Suplemento 180. Quito, Quito, Ecuador.

El Comercio. (2016). Supuestos hackers podrían recibir hasta cinco años de cárcel. Recuperado de http://www.elcomercio.com/actualidad/hackers-senescyt-titulosfalsos-licencias-carcel.html

HerramientasInformaticas. (s.f.). Obtenido de http://www.ordenadores-y-portatiles.com/herramientas-informatica-forence.html

Gratton, P. Protección informática, Editorial Trillas, 1° Edición, México, 1998, pág. 23.

Morón Lerma, Esther: "Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red", Editorial Aranzandi, Segunda Edición, Navarra, 2002, Pág. 25.

Policia Nacional del Ecuador, (2017). Delitos informáticos establecidos en el COIP y cómo prevenirlos. Obtenido de http://www.policiaecuador.gob.ec/

Quiroz Cuaron, Medicina Forense. Porrúa, México, 2002.

Registro oficial. (22 de marzo de 2018). fielweb: https://www.fielweb.com/Index.aspx?uiea#app/buscador

Riquert, Marcelo Alfredo: "Informática y Derecho Penal Argentina", Editorial Ad-Hoc, 1° Edición, Buenos Aires, 1999, pág. 21.

Seguros_informaticos. (2009). www.segu-info.com.ar. Obtenido de http://www.segu-info.com.ar/ataques/ataques.htm

Taborda, K. Branco, J., Cardoso, J., El uso de la informática en la pericia criminal y sus herramientas. *Revista Espacios*. Vol. 38, Año 2017. Número 51 Pág. 25 Recuperado de: http://www.revistaespacios.com/a17v38n51/a17v38n51p25.pdf

Todoecommerce. (2018). Ataques Informáticos: Principales Problemas De Seguridad. Obtenido de http://www.todoecommerce.con/ataques-informaticos.html.

Vargas Alvarado, E. Medicina Forense Y Deontología Médica: Ciencias Forenses Para Médicos Y Abogados, Trillasméxico, 1991.

1. Abogado, Magister en Diseño Curricular, PhD(C) en Ciencias Jurídicas en la Pontificia Universidad Católica de Argentina (UCA), Coordinador Académico y Docente Titular de la Facultad de Derecho y Gobernabilidad de la Universidad Tecnológica ECOTEC. calcivar@ecotec.edu.ec

2. Ing. Estadístico e Informático, Magister en Administración de Empresas, PhD(C) en Ciencias de la Educación en la Universidad de la Habana (UH), Coordinadora de Información y Estadísticas de Vicerrectorado Académico y Docente Titular de la Facultad de Sistemas Computacionales de la Universidad Tecnológica ECOTEC. gblanc@ecotec.edu.ec

3. Ing. Estadístico e Informático, Especialista En Proyectos De Desarrollo Educativos y Sociales, Magister En Educación Superior, Master en Análisis Avanzado de Datos Multivariantes, PhD(C) en Estadística Multivariante Aplicada en la Universidad de Salamanca España (USAL). Docente Titular de la Facultad de Ciencias de la Salud de la Universidad Estatal de Milagro (UNEMI). jcalderonc@unemi.edu.ec