Recibido: 21 octubre de 2018 / Aceptado: 23 de febrero de 2019
Conference Proceedings UTMACH V.3 Núm.1 (2019)
ISSN: 2588-056X

Análisis y revisión sobre delitos informáticos en el Ecuador

Analysis and review of cybercrimes in Ecuador

González Sánchez Jorge
Universidad Técnica de Machala / jgonzalez@utmachala.edu.ec
Machala - Ecuador

Hidalgo Romero Cristian
Universidad Técnica de Machala / chidalgo_romero@hotmail.com
Machala - Ecuador

Arce Rodríguez Juana
Universidad Técnica de Machala / jarce@utmachala.edu.ec
Machala - Ecuador

Ordoñez Barberán Plutarco
Universidad Técnica de Machala / rojofraty@gmail.com
Machala - Ecuador

Versión electrónica
https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/issue/view/3

RESUMEN

Este trabajo aborda una revisión teórica contractual sobre los fraudes informáticos y delitos competentes en el uso de sistemas gestados en ordenadores, de manera particular se enfoca en el "phishing" y el "pharming" como principales tipos de estafa; también se enmarca un análisis crítico de tendencia objetiva sobre la legislación ecuatoriana entorno a esta temática, cuales artículos constitucionales, políticas y leyes conjugan el debido proceso acerca de estos casos para medir cualitativamente hasta donde la nación ostenta dichos percances, a la vez que se citan casos estipulados a nivel regional; además, se argumentan con estudios de derecho afines que exhiben una revisión penal sobre delitos informáticos documentados, desde una perspectiva general se estima a nivel macro, meso y micro información interesante del tema que arroje secuencialmente los postulados para determinar el estado de la problemática, bajo la finalidad de diagnosticar las mejores medidas a tomar para contrarrestar sus efectos en la sociedad de la información, desde el punto de vista cognitivo se compara otros percances acordes al tema central a modo de inspección dando pautas donde se evidencia las potencialidades de prepararse contra ciberdelitos en la adecuación tecnológico y socioeconómico tanto para entidades públicas y como privadas.

Palabras clave: Delitos informáticos, phishing- pharming, legislación.

ABSTRACT

This paper deals with a contractual theoretical review of computer fraud and computer-related crime in the use of systems based on computers, in particular focuses on "phishing" and "pharming" as main types of scam; also fits a critical analysis trend objective on Ecuadorian legislation environment to this subject, which refers to articles constitutional, political and law, spouse due process about these cases to measure qualitatively where the nation holds such mishaps, while the cited cases stipulated at the regional level; In addition, related that exhibit a review argue with law studies criminal on documented, from a general perspective cybercrime is estimated at macro level, meso and micro interesting information in the topic sequentially throwing the postulates to determine the State of the problem, under the purpose of diagnosing the best measures to counter its effects in the information society, from the cognitive point of view compared with other additional conditions to the central theme as ofthe destruction of electric power the technological and socio-economic suitability for public entities and private.

Keywords: Ofesess computer, phishing-pharming, legislation.

Introducción

Hoy en día se vive la era de la información implantada mediante la sociedad del conocimiento misma que otorga nuevas facilidades, mejores prestaciones e integra nuevas metodologías en el accionar de los hechos, estas ventajas también favorecen el desarrollo del crimen gracias al auge de los sistemas digitales, por lo tanto el actuar jurídico se enfrenta a una serie de penalidades nunca antes vistas mismas que han llamado la atención y revolucionado la seguridad pública-privada e incluso la personal a nivel simbióticos con la tecnología. La tipificación de las leyes nacionales da un instrumento para accionar en contra de delitos, pero su desconocimiento general sumado a su corto alcance converger en un sistema vulnerable desde las prestaciones informáticas hasta la falta de responsabilidad del proceso como tal, lo que se traduce en varios casos sin solventar. (TOLEDO, 2016)

La complejidad de los delitos informáticos muchas veces no radica en las habilidades tecnológicas ni mecanismos informáticos, sino en los accionantes que motivan dicho acto, en Japón un estudio determina que la mayoría de estos actos son por satisfacción personal demostrar su potencial a sí mismos, lo cual indica que se deben efectuar estudios psicológicos referentes a los ciberdelincuentes que linealicen su dominio entorno al sistema social y su conducta como acto ilícito mal intencionado (Kishi, Suzukri, Monma, & Takeda, 2018). Una falencia grave es el descornamiento sobre las leyes donde acogerse en la materia de ciberdelitos, también lo es la falta de una normativa nacional que regule, penalice e interprete correctamente las bondades Cloud Computing en el Ecuador,

además de ejercer un medio clave para impulsar tanto el desarrollo penal como tecnológico a nivel regional. (Sánchez, 2017)

En el marco nacional se limita principalmente a análisis de los artículos 190, 234 y 234 del COIP que son competentes a legislar los delitos informáticos y medios electrónicos con fines fraudulentos, a pesar de ello están encaminados pero se evidencia una insipiencia en su alcance sumada a una falta de dinámica para su respectiva aplicación que no acomete adecuadamente el debido proceso por parte del denunciante, pese a ello se estudia su incidencia filtrada por la opción de jueces, fiscales y abogados cuya trayectoria les permite compilar criterios acerca de la problemática.

Materiales y Métodos

Dentro de los delitos informáticos se presentan las formas más significativas de fraudes las cuales se centran en la obtención de datos privados o la suplantación de identidad de una víctima, por lo general las fórmulas empleadas por el software espía para propagarse son los virus troyanos o los más conocidos como bombas lógicas que se descarguen a través del internet los cuales se instalan de manera automática en el PC y son procedentes de páginas o secciones poco fiables. De esta manera el defraudador obtiene la información de la víctima los datos bancarios y claves relevantes de la víctima para en un futuro utilizarlas y proceder a la realización de transferencias y desembolsos sin el consentimiento de la víctima.

Obtención de datos de la víctima sin que ésta se percaté de que se la está enviando al defraudador (PHISHING).

En la actualidad la mayoría de los casos de fraudes corporativos se han detectado por suplantación de imagen corporativa mediante las siguientes metodologías:

- Páginas dedicadas a la venta de productos en línea.
- Venta de recargas de móviles con tarjeta de crédito.
- Encuestas falsas son plantadas por organismos oficiales ilícitos.

Una forma derivada del Phishing se denomina Pharming, ésta se encarga de manipular las direcciones del DNS y redireccionar a los usuarios a páginas que ellos desean ver, pero estas páginas están suplantadas y son fraudulentas, se consiguen que las personas autentifiquen sus datos en las compras online y lo realizan mediante un pequeño archivo llamado Host. (TERUELO, 2007)

Estado de la Problemática a nivel social, criminal y judicial en ámbito Internacional A nivel global existen académicas orientadas a la formación profesional contra la delincuencia enseñando criminalista avanzada, técnicas y procesos complejos para aprender a combatir los males sociales derivados de los actos ilícitos, en los últimos 20 años se han insertado un nuevo tipo de ataques denominados delitos informáticos cuya mayor percance no son las prestaciones tecnológicas ni la brecha de conocimientos entre el hacker-agentes, sino la falta de preparación practica que no linealiza el proceder ni accionar en función de la taxonomía de los ataques independientemente de su medio, por ello se propone una formación experimental en criminología informática con el afán de mejorar la respuesta frene a tales acontecimientos. (Brooke Nodeland, 2018)

Dentro de la sociedad contemporánea se exhiben discrepancias entre la policía y los delitos informáticos en especial los orientados a la suplantación o cambio de identidad, no solo en redes sociales ni documentos de identidad, sino en sitios web, agencias bancarias e inclusive agentes del gobierno propiciados por motivos políticos, la discrepancia es que existe un brecha entre actuar público-policial derogando el actuar de la seguridad informática de manera individual en lugar de propinar normativas nacionales de control. (Wall, 2013)

La figura 1 esquematiza la estructura de los cibercrímenes y facilita su respuesta en base a las autoridades competentes.

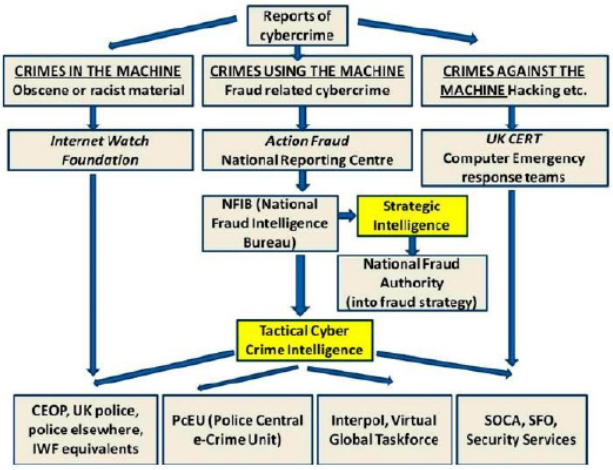

Fig. 1. Estructuración de cibercrímenes en departamento de policía del Reino Unido
Fuente: (Wall, 2013)

En el ámbito judicial se estudian modificaciones dinámicas a las leyes que regulan los actos ilícitos mediante ordenadores, sistemas ofimáticos u otro medo digital, en Venezuela se propone una Inter operatividad conjunta entre municipalidades-gobierno nacional donde la información esté al alcance de todos y protegida por fases escalables desde los funcionarios hasta los usuarios evitando así fugas de datos por parte de extraños que no forman parte del sistema; se aplica el método de la Pirámide de Kelsen para proponer y reforzar de manera interactiva las falencias en sus sistema judicial. En la figura 2 se aprecia un diagrama de flujo que esquematiza el modo de actuar frente a connatos informáticos

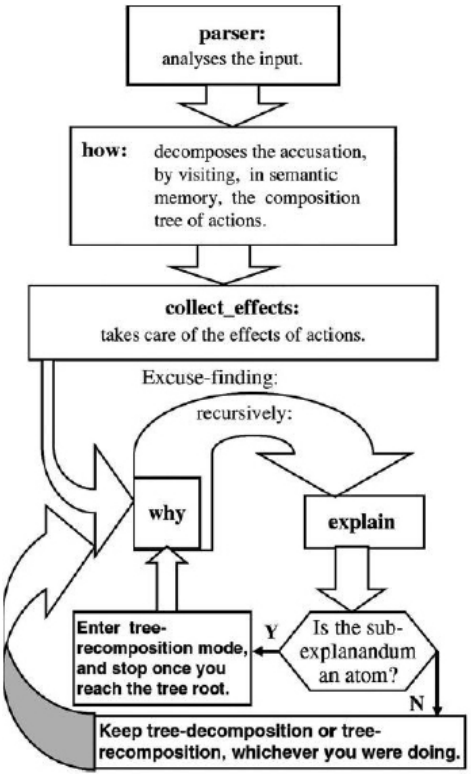

Fig. 2. Diagrama de flujo sobre accionar frente delitos informáticos
Fuente: (Giudice, 2017)

En el medio profesional de la banca pública y privada se acentúa una notable diferencia entre seguridad percibida y seguridad prestada, se debe centrar en el sentir de las personas educarlas para que sepan como identificar protegerse a la vez que se sientes seguros de sus transacciones, por ende en su vida cotidiana conviven con la tecnología, mientras que la seguridad prestada es la que existe en medios virtuales de las páginas web, mecanismo bancarios o procesos controlados de identificación, pero esto no garantiza una adecuada protección debido a que la falta de conciencia sobre capacitación de seguridad crea puertas para el accionar mal intencionado. (Garry White, 2017)

Las ciencias judiciales a nivel global están evolucionando para tratar sobre problemas informáticos que datan desde pérdida de información en ordenadores hasta sistemas virtuales de trabajo gestados en Cloud Computing, las indagaciones apuntan hacia la instauración de convenios, tratados y estándares internacionales que rijan la escabilidad del trato a información de forma penal homologando delitos -castigos. (LUX, 2017)

Varios enfoques predictivos derivados de inteligencia artificial para prevenir los daños del litigio, siendo el software ALIBI que se encarga de tomar decisiones en sitios web buscando ser un juez virtual con la finalidad de personificar a alguien acusado generando explicaciones alternativas coherentes para denegar una responsabilidad menor para luego implementar una ley, se piensa que a futuro podrían gestar acciones bursátiles y asistencia a las Pymes bajo un razonamiento transparente, lógico e imparcial. (Nissan, 2018)

Análisis judicial sobre los delitos informáticos en el Ecuador Tipificación:

En un estudio efectuado a 30 personas inmersas en el ejercer de derecho se determinó que las principales falencias denotadas son la falta de socialización entorno a la comunidad sobre la existencia de las leyes y artículos panales afines a derechos informáticos que a pesar de existir denuncias no se toma enserio el caso o el delincuente sale libre por la falta de un debido proceso acorde al castigo legal. La no adecuación de conductas nocivas basadas en ordenadores en código penal hace que la mayoría de casos se cataloguen como cifras negras, también se hace notoria que la distribución de denuncias sea 54% a fraudes-robos, 40 % virus o gusanos y 6% pedófilos o acosadores. El 99% considera que las leyes nacionales deben ser mejoradas por considerarse insuficientes en materia informática haciendo hincapié en la capacitación a autoridades seccionales, notarios y abogados, debido a que la población considera que las TIC´s se han transformado en un arma poderosa al infringir la ley, no obstante el problema base no son las prestaciones tecnológicas sino la falta de presupuesto económico para desarrollar estrategias que eviten tales connatos.(Tacuri, 2012)

Hacker como sujeto activo: El hacker como sujeto penal no ha sido clasificado ni debidamente identificado desde la perspectiva penal, en el Ecuador se han dado casos excepcionales de Hacking como el de Villavicencio y WikiLeaks donde se divulgo correos gubernamentales con información categorizada como secreto de estado, a pesar de ello se privó de libertad a Villavicencio mientras que Assange se alojó en nuestra embajada bajo decreto presidencial aun sin un análisis jurídico competente, ha habido casos como terrorismo informático de Anonymo us en el 2010 que revelo la decorosa vida de los funcionarios de Correa, aún bajo tales circunstancias nada se pudo hacer debido a la preparación y casi nula respuesta por parte de los dirigentes estatales y responsables de la seguridad nacional, también se presentó casos de Phishing y carding a bancos ecuatorianos sin que se puede detectar al hackers; por ello se deduce que la principal falencia es la falta de profesionales capaces de actuar ante delitos informáticos debido a la mala telemática que rige los sistemas digitales en el país. (LOAIZA, 2017)

Telecomunicaciones: Se hace notoria la falta de asociación a convenios internacionales sobre la problemática privan al país de las herramientas y saberes competentes al actuar en respuesta a delitos informáticos, se evidencia que la mayoría de casos registrados no

son tratados debido a la poca interpretabilidad de jueces, que sumada al desconocimiento general resulta en la impunidad, la mayoría de empresas prefiere no denunciar por miedo a dejar en visto su falta de seguridad, también que los delincuentes comunes se diferencia de los hackers en las facilidades con la cual estos manipulan sistemas digitales, como medida se opta por contratar a hacker éticos que entregan informes sobre el nivel-estado de seguridad de empresas diseñando medidas de seguridad para tales entidades. (LLANGARÍ & ANDRÉS, 2016)

Redes Sociales: Al ser un medio masivo de interacción social se han trastornado en el medio propicio para desarrollar nuevas formas de estafa e ilícitos, la mayoría de las personas encuestadas considera que se debe sancionar a quienes suplantan perfiles, se apropian de cuentas o divulgan información sensible en Facebook, no se sientes protegidos por la ley ni saben si dichos actos son o no motivo de actuar legal. Existe un desinterés social a nivel nacional sobre penalizar los delitos informáticos sin medir el riesgo tras sus facilidades frente a la vida personal de cada usuario. (Paola, 2014) Código Orgánico Integral Penal: Se entrevistó jueces, fiscales y abogados dando las siguientes observaciones:

- Se considera que existe conformidad con la cantidad de artículos, pero no su correcta interpretación y aplicación.
- Se considera que existe un nivel regular en cuanto al dominio de la temática en los tribunales debido a los pocos casos procesados contra los no procesados (impunes).
- Hace falta una ley nacional para asuntos relacionados al Cloud Computing, asi como exigir políticas internas de cada empresa en concordancia con el accionar administrativo-legal.
- Los artículos 190, 232 y 234 deben perfeccionarse para suplir sus falencias, discrepancias y poca adaptabilidad a complicaciones prácticas. (TOLEDO, 2016)

El Ecuador debe adherirse a convenios internacionales y compararse con leyes globales de protección en sistemas informáticos para retroalimentar-actualizar material penal, judicial y técnicas en casos denunciados, en ciertos casos a pesar de haber identificados los daños se carece de los medios o saberes para encontrar al hacker ni como tomar medidas entorno al uso indebido de malware, ni la policía ni fiscalías cuentan con la tecnología de vanguardia necesaria en tales casos, por ende se han dado casos de suplantación de identidad a bancos o usuarios estatales que han quedado sin sentencia por la falta de interpretabilidad y medios para capturar al delincuente; en contraste con casos de Villavicencio, Anonymo us, WikiLeaks existen leyes pero solo se privó de libertad al ecuatoriano debido a que los otros casos son de índole internacionales. (Jácome, 2016) La tabla 1 muestra un resumen del análisis efectuado a las leyes nacionales proponiendo mejoras a partir de las falencias detectadas.

Tabla 1. Análisis de artículos en COIP nacional

ARTÍCULOS	ALCANCE	VULNERABILIDAD	MEJORA
190	Apropiación fraudulenta por medios electrónicos	Falencias en aplicación de sanciones e identificación de activos	Describir posibles casos e integrar uso de software como agente de daño cuya responsabilidad es del usuario.
232	Ataque a la integridad de sistemas informáticos	El sujeto activo es cualquier persona con o sin saber de informática, sujeto pasivo es el sistema informático.	Identificar de mejor manera el accionar tanto al estado, sociedad, cuerpo policial y establecer medidas legales más claras.
234	Acceso no consentido a un sistema informático, telemático o de 6 telecomunicaciones	Dirección subjetiva de la intencionalidad legal de la persona que comete el delito.	Estipular mejor las conductas tanto del sujeto activo como usuarios, cuestiones subjetivas como solo intrusión establecer sanciones administrativas no penales.

Fuente: Elaboración propia

Técnicas para combatir delitos informáticos

En el marco mundial los ciberdelitos son un tema relevante dinámico e intuitivo que constantemente amalgama nuevos recursos digitales para hacer uso indebido de las redes, por lo cual se enfatizan estudio sobre metodologías que contrarresten sus daños al prójimo, entre los más destacados se tiene:

Barrera de Cinco Niveles: Se basa en un esquema hibrido que opera en tiempo real para detectar ataques de phishing, no solo detecta el ataque en sitios web, sino que también identifica el dominio objetivo del phisher; sus características heurísticas se extraen de sitios web sin intervención de usuarios mediante JSoup. (Kalra D. K., 2016) Configuración "fast flux": Hace un cambio rápido y repentino de dirección IP asignando múltiples nombres al dominio de un servidor, alternando sus identificaciones en sus recursos, de esta forma los ciberdelincuentes ejecutan ataques colaborativos para insertar un malware o ingresar a un servidor donde hurtan la información, dicho proceso es tan rápido que dificulta mucho notar el ataque hasta que ya es demasiado tarde, no obstante también podría convertirse en una importante herramienta para protegerse de ataques informáticos si es implementado en servidores Cloud que a más de resguardar información en la nube redireccionaran los ataques a direcciones falsas. (Zhou, 2015) Contraseñas de un solo uso basadas en el tiempo: Mediante una aplicación Android o plataforma Windows se diseñó un programa que crea contraseñas únicas en un lapso de tiempo útil de 30 segundos, emplea la hora del reloj del procesador como elemento de cálculo aleatorio OTP y luego utiliza un temporizador para limitar la usabilidad, de esta forma optimiza la seguridad personal y corporativa vía msm, Hotmail, Gmail u otro medio electrónico a bajo costo sin procesos complejos. La figura 3 muestra una captura de las claves generadas on time. (Awasthi, 2015)

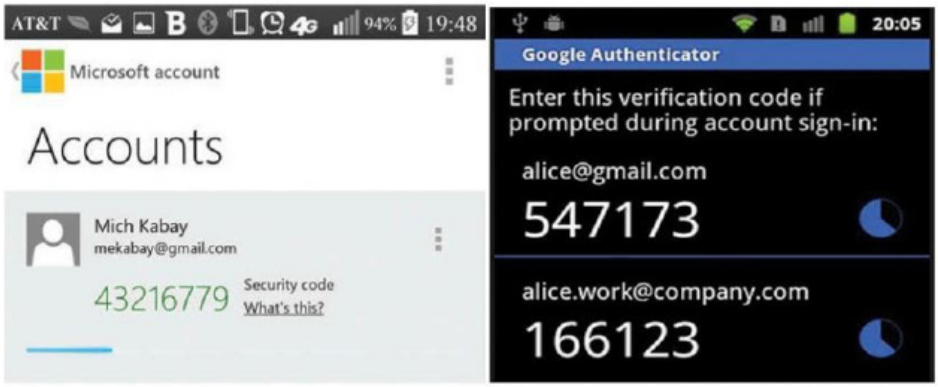

Fig. 3. Contraseñas generadas en rangos de tiempo útiles Fuente: (Awasthi, 2015

Resultados

La protección ecuatoriana entorno a delitos informáticos es de carácter regular baja, inclusive se podría categorizar como deficiente, por falencias en su interpretabilidad, insuficiencia en su aplicación, sanciones bajas inclusive en contraste con normativas de Perú, Argentina, Colombia y Venezuela notando que el país está atrasado en materia legal, judicial y técnica sobre el debido proceso en connatos informáticos. También se evidencia la falta de pericia en la formación académica, criminalista e informática para establecer procesos o criterios de respuesta frente a dichos delitos, se propone la creación de una especialidad que conjuga sistemas informáticos con asuntos penales para reforzar no solo la seguridad estatal sino social considerando tales problemas como asunto nacional en lugar de ser derogados de forma personal. Adicionalmente se identificó que la naturaleza de los delitos informáticos es de carácter psicológico mal fomentada en la falta de cultura, debido a esto se debe integrar criterios penales basados en apreciaciones tanto objetivas como subjetivas basados en los perfiles registrado de delincuentes informáticos como el caso de Japón que aprende de cada sucede de forma imparcial facilitando la ejecución de la ley o modificándola si es necesario con el fin de salvaguardar la seguridad de sus comunidades; aunque no se tiene el grado de conocimiento entorno a profesionales para diseñar sistemas de seguridad tanto públicos como privados se puede contratar a especialistas que dirijan dicha tarea y en base a ello mejorar las leyes existentes, a más de aprovechar bondades Cloud bajo un reglamento local que permita su distribución y control. Puesto que el recurso tecnológico es automatizable, imparcial lógico, la falencia radica en la parte humana que supervisa dicho sistema, por cual su falta de saberes o capacidad de respuesta da como resultado un delito impune. La tabla 2 expresa una matriz FODA sobre el estado nacional entorno a los delitos informáticos.

Tabla 2. Análisis FODA sobre delitos informáticos a nivel nacional

	Fortalezas: Leyes establecidas, recursos tecnológicos, profesionalidades afines, cambio cultura y desarrollo empresarial y social entorno a la informatica	**Debilidades:** Pocos saberes y recurso humano capaz de enfrentar delitos informatico, no se concatena profesiones para solucionar problemas latentes, poco recurso económico y esfuerzo politicos para mejorar la situación estatal
Oportunidades: Mejorar la estructuración de leyes, escabilidad e integrar patrones adecuados de conducta legal- penal. Gestar desarrollo privado-público en sistemas digitales y virtuales bajo normas de seguridad aptas.	Alianzas internacionales a convenios para llenar el vacío legal nacional, aprender de estudios extranjeros y traer personal que diseñe, enseñe seguridad informática	Derogar esfuerzos nacionales, designar presupuesto para capacitación de jueces, abogados e ingenieros de sistemas para reforzar la seguridad social.
Amenazas: Hackeos a bancos, empresas, entidades públicas Delitos impunes por vacíos legales o negligencias penales	Desarrollar normativas locales, regionales de carácter flexible y dinámico para usar recursos Cloud e importar tecnologías de vanguardia, así como editar leyes en base a casos registrados.	Crear académicas de criminalística que formen al cuerpo policial para responder adecuadamente frente a delitos informáticos y su actuar sea acorde al debido proceso judicial.

Fuente: Elaboración Propia

Conclusiones

Implementar mejoras al sistema judicial tanto público como privado mediante uso de inteligencia artificial, softwares de control; así como medidas tanto físicas como lógicas a los funcionarios, a más de promover un cambio en la mentalidad nacional para tomar en serio a los delitos informáticos desde un punto de vista tanto penal como moral en el eje de desarrollo social, también se puede amalgamar los objetivos de crecimiento económico en virtud de las mejores prestaciones tecnologías asumiendo el riesgo permisible de empresas y bancos.

Se aconseja designar un presupuesto estatal enfocado a crear un ministerio que regule específicamente los delitos informáticos y en base a tal estudio proponer mejoras en la seguridad nacional, local e inclusive de empresas, dando sustento legal a las políticas administrativas internas bajo sanciones contempladas en la ley; llenar los vacíos legales con acuerdos internacionales a través de una mejor preparación tanto humana como tecnológica para responder adecuadamente a dichos percances

Referencias Bibliográficas

Aguilar, E., Cuamatzi, A., & Sánchez, J. (2009). Phishing Amenaza y Factor de Riesgo en las tecnologías de la imformación del mundo empresarial. México D.F: Instituto Politecnico Nacional.

Awasthi, A. (2015). Reducing Identity Theft Using One-Time Passwords and SMS. The EDP Audit, Control, and Security Newsletter, 9-19.

Borrero, R. C., Rojas, J. A., & Montes, J. J. (2015). La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. Rev. Derecho comun. Nuevas tecnol. N°14, 1-26.

Brooke Nodeland, S. B. (2018). Teaching Cybersecurity to Criminal Justice Majors. Journal of Criminal Justice Education,, 1-20.

Colaguori, C. (2012). Computer crime, investigation, and the law,. Police Practice and Research, 539-540.

Ezhil Kalaimannan, S. K. (2017). Influences on ransomware's evolution and predictions for the future challenges,. Journal of Cyber Security Technology, 23-31.

Ferruzola Gomez, E. C. (2014). Cómo responder a un Delito Informático. . UNEMI, 44- .

Garry White, T. E. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. Journal of Computer Information Systems, 353-363.

Gascón, Y., Aguilarte, E., Cafaro, R., & Pérez, B. (2014). Análisis jurídico del gobierno electrónico en el marco de la interoperabilidad entre los Consejos Comunales y la Alcaldía de Maturín-Venezuela. Revista Venezolana de Información, Tecnología y Conocimiento, 66-85.

Giudice, M. E. (2017). DATOS EMPRESARIOS, PROTECCIÓN EN LA ACTUAL SOCIEDAD DE LA INFORMACIÓN: UNA VISIÓN ARGENTINA. Rev. Derecho comun. Nuevas tecnol. No. 17, 1-21.

J.G, F. T. (2007). Respuesta Penal Frente a Fraudes. Derecho Penal y Criminología, 218- 220.

Jácome, R. P. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. QUITO: UNIVERSIDAD CENTRAL DEL ECUADOR.

Kalra, D. K. (2016). Five-tier barrier anti-phishing scheme using hybrid approach, Information Security. Journal: A Global Perspective, 247-260.

Kishi, K., Suzukri, J., Monma, T., & Takeda, T. A. (2018). Psychosocial and criminological factors related to recidivism among Japanese criminals at offender rehabilitation facilities. Cogent Social Sciences, 1-32.

Kranenbarg, M. W., & Gelder, T. J.-L. (2017). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only,

LUX, L. M. (2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. Revista Chilena de Derecho,, 235-260.

Nissan, E. (2018). Computer Tools and Techniques for Lawyers and the Judiciary. Cybernetics and Systems, 201-233.

Oxman, N. (2013). Estafas Informátias a través de Internet. Revista de derecho de la Pontifica Universidad Católica de Valparaíso XLI, 211-262.

Paola, C. B. (2014). La apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación

del delito informático en la legislación penal ecuatoriana. QUITO: UNIVERSIDAD CENTRAL DEL ECUADOR.

Pino, A. D. (2009). Informática Forense en el Ecuador. Quito: FISCALIA GENERAL DEL ESTADO.

POLICIA NACIONAL DEL ECUADOR. (s.f.). Délitos Imformáticos o Ciberdélitos. Obtenido de http://www.policiaecuador.gob.ec/delitos-informaticos-o- ciberdelitos/

Sánchez, J. G. (2017). Analisis regulatorio y comercial para el desarrollo de servicio de cloud computing para la provincia de El Oro-Ecuador. T. Machala: Espol.

Tacuri, A. J. (2012). Los Delitos Informáticos y su Tipificación en la Legislación Ecuatoriana. LOJA: UNIVERSIDAD NACIONAL DE LOJA.

TERUELO, J. G. (2007). RESPUESTA PENAL FRENTE A FRADUDES. REVISTA DE DERECHO PENAL Y CRIMONOLOGÍA, 218-220.

TOLEDO, D. W. (2016). ANÁLISIS DE LOS DELITOS INFORMÁTICOS POR ATAQUE Y ACCESO NO AUTORIZADO A SISTEMAS ELECTRÓNICOS, TIPIFICADOS EN LOS ARTÍCULOS 232 Y 234 DEL CÓDIGO ORGÁNICO INTEGRAL PENAL EN EL ECUADOR. QUITO: Universidad Católica de Santiago de Guayaquil.

Trejo, A., Alvarez, D., & Chimbo, O. (2015). La seguridad Juridica frente a los delitos i mformáticos. Investigación Jurídica, 43-44.

Wall, D. S. (2013). Policing identity crimes, Policing and Society,. Policing and Society, 437-460.

White, G., & Visinescu, T. E. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. Journal of Computer Information Systems, 353-363.

Zhou, S. (2015). A Survey on Fast-flux Attacks. Information Security Journal: A Global Perspective, 79-97.

CURRÍCULUM DE LOS AUTORES

1 Jorge Luis González Sánchez
Cédula de identidad: 072938959
Ciudad: Machala País: Ecuador Estudios:
Educación Cuarto Nivel
Universidad "Escuela Superior Politécnica del Litoral" (ESPOL)
Maestría en Telecomunicaciones
Educación Tercer Nivel
Universidad "Escuela Superior Politécnica del Litoral" (ESPOL)
Ingeniería en Electrónica Y Telecomunicaciones
Experiencia Laboral: Docente Investigador y de la Unidad Académica de Ciencias Empresariales de la Universidad Técnica de Machala

2 Cristian Hernán Hidalgo Romero
Ciudad: Machala País: Ecuador Estudios:
Educación Cuarto Nivel
Universidad Internacional de la Rioja UNIR España Maestría en Dirección y Gestión Sanitaria (En curso) Educación Tercer Nivel
Universidad Estatal de Guayaquil
Experiencia Laboral: Hospital IESS Machala como Médico Auditor de la Institución desde el mes de Mayo del 2018 hasta la presente fecha

3 Juana Juliana Arce Rodríguez
Cédula de identidad: 0703771998
Ciudad: Machala País: Ecuador Estudios:
Educación Cuarto Nivel
Universidad Nacional de Piura
Maestría en Seguridad Industrial, Salud Ocupacional y Relaciones Comunitarias.
Educación Tercer Nivel Universidad Técnica de Machala Licenciada en Enfermería Experiencia Laboral:
Docente de Nivelación y Admisión de la Universidad Técnica de Machala Docente de la Unidad Académica de Ciencias Químicas y de la Salud de la
Universidad Técnica de Machala