Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VII Número: Edición Especial Artículo no.:140 Período: Diciembre, 2019.

TÍTULO: Desafío de la ciberseguridad ante la legislación penal.

AUTORES:

1. Máster. Frankz Alberto Carrera Calderón.
2. Ing. Joel Estuardo Quilligana Barraquel.
3. Máster. Mario Danilo Aguilar Martínez.
4. Máster. Santiago Fernando Fiallos Bonilla.

RESUMEN: En el año 2019, Ecuador ha sido blanco de una gran cantidad de ataques a sus sistemas informáticos públicos, debido a que el Estado ecuatoriano dejó de dar asilo político, al señor Julían Asange; esto permitió que especialistas en el área del derecho como en el de la seguridad informática, establezcan una discusión sobre los aspectos importantes como ciberdelitos, ciberseguridad, ciberespacio y la normativa jurídica cuando se enfrenta a delitos informáticos.

PALABRAS CLAVES: ciberseguridad, delitos informáticos, Ecuador, ciberdelitos, cibercrimen.

TITLE: The challenge of cyber security before criminal legislation.

AUTHORS:

1. Máster. Frankz Alberto Carrera Calderón
2. Ing. Joel Estuardo Quilligana Barraquel
3. Máster. Mario Danilo Aguilar Martínez
4. Máster. Santiago Fernando Fiallos Bonilla

ABSTRACT: In 2019, Ecuador has been the target of a large number of attacks on its public computer systems, because the Ecuadorian state stopped giving political asylum to Mr. July Asange, this allowed specialists in the area of law as in the area of informatic security establish a discussion on important aspects such as cybercrime, cybersecurity, cyberspace and legal regulations when dealing with cybercrime.

KEY WORDS: cybersecurity, computer crimes, Ecuador, cybercrime, cybercrime**.**

INTRODUCCIÓN.

Los días subsiguientes al anuncio por parte del gobierno ecuatoriano de retiro del asilo político a Julián Assange, Ecuador sufrió una cantidad de ataques a cibernéticos, según el periódico El Comercio de la ciudad de Quito se registraron "más de 40 millones de ataques dirigidos por piratas informáticos" (El Comercio, 2019). Estos ataques fueron ejecutados desde ocho países, Reino Unido, Francia, Holanda, Alemania, Austria, Estados Unidos, Ecuador y Rumanía.

El periódico Expreso de la ciudad de Guayaquil manifestó que hasta el 11 de abril del 2019, día en que fue anunciado el retiro del asilo político, Ecuador estaba "en el puesto 55 del ranking de los países más vulnerables en el mundo y luego ocupó el número 25 en menos de cuatro horas" (Expreso, 2019), según datos de la empresa en seguridad informática Kaspersky.

De las varias modalidades que normalmente usan los hackers, la más utilizada para el ataque a las instituciones públicas ecuatorianas "fue saturar los sitos de Internet y sobrecargarlos de información para que los usuarios no pudieran usarlos" (El Comercio, 2019b), es decir, llenar los servidores de las instituciones públicas con pedidos de actividad, siendo esta una de las formas más básicas de ataque.

Una de las principales redes de hackers que se involucró en este ataque fue la denominada red "Anonymous". Las principales entidades atacadas fueron Banco central, Presidencia, Cancillería, Consejo de la judicatura, Ministerio del Interior, SRI, CNT, gobiernos autónomos.

El periódico El Comercio el 15 de marzo del 2018 en su artículo periodístico denomina-do “Banda hackeó el sistema informático de la ANT para emitir 15.000 licencias ilegales” menciona que un grupo de delincuentes obtuvo las claves de acceso de los funcionarios de la Agencia Nacional de Tránsito, lo cual les permitió otorgar más de 15.972 licencias de conducir, borrar más de 14.000 infracciones tránsito y aumentar 26.802 pun-tos a usuarios que requirieron los servicios de estos presuntos hackers. Los presuntos hackers ofertaban sus servicios a través de redes sociales tales como Facebook y Twitter. Se considera que 99 usuarios externos vulneraron en dos meses el sistema informático de la ANT. Además, se considera que 1’250.000 dólares movió la red delictiva.

Una supuesta banda de hackers atacó y violentó las seguridades del Sistema de Registro de Títulos de la Secretaria Nacional de Educación Superior en el año 2016 y como resultado entregaron 366 títulos universitarios falsos.

De acuerdo a la empresa especialista en seguridad informática Centurylink en Ecuador se registran: a) de 10 a 12 ataques informáticos por segundo; b) la mayor parte de ataques cibernéticos que recibe Ecuador proviene de China, Estados Unidos y Brasil; c) en Ecuador no hay legislación para sancionar la suplantación de identidad digital; c) El daño provocado por los ciber ataques llegaría a 6 trillones de dólares hasta el 2021; d) el robo de información personal, empresarial o gubernamental es el delito más común en el país.

Según el último estudio del 2018 realizado por la empresa especializada en seguridad informática McAfee dio como resultado que la cibercriminalidad cuesta unos US$ 600,000 millones al año en todo el mundo (McAfee, 2018).

La presencia de delitos informáticos en el Ecuador es muy notoria, por lo cual han surgido métodos de defensa y profesionales en el área de la ciberseguridad, para contrarrestar el visible peligro al que está expuesta nuestra información y la integridad de la misma.

Esto marcó claramente la dimensión del riesgo al que está expuesto el país en el área de seguridad de la información, teniendo en cuenta que el riesgo se mide en función de la probabilidad e impacto del ataque cibernético, surgen una serie de preguntas: ¿existe normativa jurídica en Ecuador para penalizar los ataques cibernéticos? ¿Cuáles son las medidas de prevención y penalidades que acarrean este tipo de actos?, ¿qué es la ciberseguridad, ciberdelito, cibercrimen, ciberespacio?, ¿Cuáles son los profesionales que trabajan para prevenir y controlar los ciberataques?

Por lo cual, el presente artículo pretende socializar tanto a los profesionales en el área de Ciberseguridad como a los juristas ecuatorianos sobre la situación jurídica actual en materia de delitos informáticos en el Ecuador, tomando en cuenta la ambigüedad de las distintas leyes que penalizan los delitos informáticos y las inconsistencias en el debido proceso.

DESARROLLO.

Métodos.

Para el desarrollo del artículo se llevó a cabo una revisión de diferentes tipos de documentos, entre los cuales se encuentran aquellos publicados en periódicos de difusión nacional, de igual manera libros y artículos científicos sobre el tema de investigación.

Se realizó un análisis fundamentado el Código Orgánico Integral Penal y los delitos informáticos y algunas de las modalidades de cometimiento del delito por parte de los delincuentes informáticos.

Resultados.

De la sistematización bibliográfica que se llevó a cabo en la investigación, se desprendió una serie de conceptos técnicos para enmarcarse en el área de estudio de este artículo, de ahí que, se define aspectos tales como: ciberespacio, ciberseguridad, además quienes son los profesionales que trabajan con la ciberseguridad.

Ciberespacio.

Según el estándar ISO/IEC 27032:2012 al hablar de tecnología de la información, técnicas de seguridad y directrices para la ciberseguridad, establece que es el "entorno complejo resultante de la interacción de personas, software y servicios en internet por medio de dispositivos tecnológicos y redes interconectadas que no existe en una forma física" (ISO/IEC, 2012, pág. 6). Se puede afirmar que el ciberespacio es el actual y poco explorado perímetro de batalla entre sociedades y estados.

Ciberseguridad.

Al tratar de definir que es la ciberseguridad, una de las organizaciones a nivel mundial de prestigio es el grupo de trabajo *Join Task Force,* mismo que define la ciberseguridad como: "Una disciplina basada en la informática que involucra tecnología, personas, información y procesos para permitir operaciones aseguradas en el contexto de adversarios. Implica la creación, operación, análisis y prueba de sistemas informáticos seguros. Es un curso de estudio interdisciplinario, que incluye aspectos de derecho, política, factores humanos, ética y gestión de riesgos" (JTF, 2017, pág. 16).

La Ciberseguridad permite tener una visión especifica de temas concretos que están relacionados con la seguridad de la información. Además, es necesario comprender que existe una marcada diferencia entre Ingeniería de Software y Ciberseguridad y es que la primera tiene como objetivo primordial hacer el software funcione de una manera eficiente y adecuado, mientras que la segunda trata de brindar la mayor seguridad al software para que incidentes de riego informático no alcancen sus propósitos.

Profesional de la Ciberseguridad.

Para (Rodríguez Canfranc, 2019), es el experto en temas de seguridad informática que cuenta con conocimientos técnicos y legales que lo respaldan a la hora de: analizar, diseñar e implementar

estrategias que permitan salvaguardar la confidencialidad, privacidad e integridad de los datos, permitiéndole brindar a los usuarios y organizaciones una infraestructura informática segura.

Los profesionales de ciberseguridad generalmente son expertos en informática, software, seguridad de redes, que realizan sus actividades basados en lo que se conoce como “hacking ético”.

Hacker.

Según el creador del sistema operativo Linux, Linux Torvalds citado por (Himanen, 2002), los hackers son expertos en informática que han dejado de usar sus computadores para obtener únicamente ingresos económicos, sino más bien lo hacen por sentido social o de entretenimiento.

El término “hacker” en sus inicios hace referencia a un grupo de expertos en programación y redes que fueron los pioneros en la creación de lo que hoy conocemos como Internet. De acuerdo al criterio de (Steven Raymond, 2001) “Los hackers resuelven problemas y construyen cosas, y creen en la libertad y la ayuda voluntaria mutua” (pág. 3). Raymond señala que existe una cultura completa desarrollada alrededor de los “hackers”, “la tarea de un hacker no es dañar, es conocer”. Este interesante concepto fue acogido por toda una comunidad de expertos, quienes tienen dentro de sus reglas (Ríos, 2003) mantener el anónima y la discreción de sus actividades.

Herramientas del profesional en ciberseguridad.

El profesional de ciberseguridad cumple sus funciones defensivas, ofensivas o simplemente de análisis de vulnerabilidades de sistemas informáticos, mediante el uso de un conjunto de herramientas cuya finalidad es fortalecer la seguridad de los mismos (Broy de la Cruz, 2013).

Entre las herramientas comúnmente utilizadas por el profesional de ciberseguridad, están aquellas denominadas “de penetración ofensiva”, mismas que le permiten aprovechar las vulnerabilidades de los sistemas informáticos de una manera ética, entre las más conocidas se podría mencionar las siguientes: Aircrack-ng, THC Hydra, Metasploit Framework, WireShark.

Cibercrimen y ciberdelito.

Para nadie es desconocido la velocidad con que se desarrolla la tecnología, y dentro del esta la informática, las telecomunicaciones e Internet han liderado dicho desarrollo. El uso que se hace de la tecnología no siempre es el adecuado para una sociedad, pudiendo aplicar la tecnología para conductas delictivas, creando la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En primer momento es necesario definir que es el delito, (Carrara, 1971) considera que el delito es "(…) aquella infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultantes de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso" (pág. 89).

Para que (Beiling, 1944) el delito es una "(…) acción típica antijurídica, culpable, subsumible bajo una sanción penal adecuada y que satisfaga las condiciones de punibilidad" (pág. 94).

El Código Orgánico Integral Penal (COIP) en su Art. 18 no define el delito, sino más bien, habla de la infracción penal y dice: "Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código" (Asamblea Nacional del Ecuador, 2014).

Sobre el mismo tema (Arroyo Jácome, 2016) considera que para que un acto sea considerado delito debe tomarse en cuenta lo siguiente:

a) El delito es un acto humano, es una acción (acción u omisión); b) dicho acto humano ha de ser antijurídico, ha de estar en oposición con una norma jurídica, debe lesionar o poner en peligro un interés jurídicamente protegido; c) debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico; d) el acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona; e) la ejecución u omisión del acto debe de estar sancionada por una pena (pág. 24).

Por otra parte, el término "ciber" según (RAE, 2019), proviene de un acortamiento del adjetivo "cibernético", es decir; que tiene relación con la tecnología y herramientas computacionales. De esta manera se podría definir al ciberdelito como: conducta típica, antijuridica y culpable en el mundo físico, cometida en el ciberespacio mediante herramientas tecnológicas y de la comunicación; mientras que el cibercrimen hace referencia a delitos informáticos más graves.

Ciberataque.

Un ciberataque es la definición que se da a una acción intencionada que inicia en equipo informático, el objetivo principal de este tipo de actos es el de comprometer la confidencialidad, disponibilidad o integridad de los sistemas, equipos, redes o sitios web atacados y a toda información que se transmite o se almacena en los mismos. El ciberataque puede tener objetivos muy variados, pero el más común y de mayor impacto, es el ejecutado por grupos hacktivistas con fines políticos. Entre los ciberataques más conocidos tenemos el ataque denegación de servicio (DoS) y el ataque denegación de servicio distribuido (DDoS), que es una ampliación del primero; estos son utilizados con la finalidad de interrumpir la correcta funcionalidad los servidores objetivo, haciendo que el recurso sea inaccesible a los usuarios legítimos (Larrieu-Let, CISM, 2015).

Situación actual de la legislación ecuatoriana frente al cibercrimen.

Ecuador no cuenta con una estructura sólida que regulen, prevenga, identifique y penalice adecuadamente los delitos informáticos en su territorio.

De acuerdo a la ministra del Interior María Paula Romo "es uno de los pocos países de la región que no cuenta con una ley para luchar contra ciberdelitos, con tecnología y personal" (El Comercio, 2019b), además mencionó que Ecuador no ha firmado ningún Convenio sobre ciberdelincuencia; sin embargo, existen ciertas leyes que penalizan este tipo de conductas, siendo el Código Orgánico Integral Penal (COIP) el principal, mismo que en su Sección Tercera "tipifica los delitos contra la

seguridad de los activos de los sistemas de información y comunicación" (Asamblea Nacional del Ecuador, 2014).

Delitos tipificados en el COIP.

A pesar que la Sección Tercera del COIP tipifica ciertos delitos informáticos, existen varios de ellos normalizados en otras secciones de este Código, a continuación, se citará dichos artículos y las posibles prácticas cibernéticas que abarcan.

Tabla 1. Delitos informáticos tipificados por COIP.

Artículo	Prácticas	(Años prisión)
Art. 103.- Pornografía con utilización de niñas, niños o adolescentes	producción edición	7 a 13
Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes	venta posesión	10 a 13
Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	grooming	1 a 5
Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos (Sexting)	sexting	7 a 10
Art. 178.- Violación a la intimidad	escuchas telefónicas	1 a 3
Art. 182.- Calumnia	calumnía	6m a 1
Art. 186.- Estafa (Carding)	carding, skimming	5 a 10
Art. 188.- Aprovechamiento ilícito de servicios públicos	robo de señal	6m a 3
Art. 190.- Apropiación fraudulenta por medios electrónicos.	cracking a redes, carding, skimming, phishing, etc	1 a 3

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles	cambio de imei cambio de Mac	1 a 3
Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles	venta base de datos	1 a 3
Art. 193.- Reemplazo de identificación de terminales móviles	cambio de correo electrónico cambio de Mac	1 a 3
Art. 194.- Comercialización ilícita de terminales móviles	venta de terminales	1 a3
Art. 195.- Infraestructura ilícita	posesión de cracks	1 a 3
Art. 208A.- Falsificación de marcas y piratería lesiva contra los derechos de autor	clonación de páginas robo de código (fin comercial)	multas
Art. 211.- Supresión, alteración o suposición de la identidad y estado civil	falsifición documentos	1 a 5
Art. 212.- Suplantación de identidad	phishing	1 a 3
Art. 220.- Tráfico ilícito de sustancias catalogadas sujetas a fiscalización	publicidad Deep web (drogas)	5 a 7
Art. 229.- Revelación ilegal de base de datos	SQL injection	1 a 5
Art. 230.- Interceptación ilegal de datos	sniffing escuchas telefónicas	3 a 5
Art. 231.- Transferencia electrónica de activo patrimonial	cashout	3 a 5
Art. 232.- Ataque a la integridad de sistemas informáticos	defacement ataque ddos posesión de herramientas (hacking) crear virus, keyloggers, spywares	3 a 7
Art. 233.- Delitos contra la información pública reservada legalmente	acceso a servidores de infraestructuras críticas	5 a 7

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	man, in the middle defacement XX's	3 a 5

Fuente: Elaborado a partir de COIP. (Asamblea Nacional del Ecuador, 2014).

Profesional de Ciberseguridad y el COIP.

Los profesionales que trabajan en ciberseguridad enfrentan desafíos y riesgos debido a que se expone a la existencia de una tipificación jurídica ambigua en el COIP en cuanto se refiere al ataque a la integridad de sistemas informáticos. Esto debido a que el Art. 232 de dicha norma jurídica estipula una serie de actividades por las cuales una persona puede considerarse que está efectuando un "ataque a la integridad de sistemas informáticos", siendo estas: destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento, comportamiento no deseado o suprimir 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.

De ahí, que las personas infractoras serían sancionadas con pena privativa de libertad de tres a cinco años.

De igual manera, el Art. 232 considera no solo a las personas que ejecutan dicha actividad, sino también hace referencia a otros actores, que: diseñen, desarrollen, programen, adquieran, envíen, introduzcan, ejecuten, vendan o distribuyan de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados anteriormente.

Considerando que las personas dedicadas a seguridad informática (hackers éticos) requieren en algún momento de su labor: diseñar, desarrollar, programar, adquirir, enviar, vender o distribuir dispositivos o programas informáticos destinados a probar niveles de seguridad de forma ética y no bajo el criterio de cometer un delito tal como lo tipifica el numeral el numeral 1 del Art. 232 del COIP.

Discusión.

En este artículo se estableció que existe un problema en cuanto se refiere a la normativa que rige los delitos informáticos y los profesionales de ciberseguridad, por cuanto, dichos profesionales podrían ser sancionados de acuerdo al Art. 232 del COIP, sin tomar en cuenta que ellos pueden ser contratados por diferentes entidades para prevenir la existencia de vulnerabilidades en sus sistemas informáticos. Es decir, la funcionalidad del sistema Judicial de Ecuador en materia de delitos informáticos es deficiente, requiriendo una reforma a dicho código.

De igual forma, el presente artículo científico identifica los escenarios y elementos que dan lugar a la aparición de conductas antijuridicas con el uso de herramientas informáticas, esto con el fin de prevenir que por desconocimiento y ambigüedad en ciertos artículos del COIP, ciertos entes judiciales puedan manipular el sistema Judicial a conveniencia y se falte gravemente al debido proceso, violentando los derechos constitucionales y mancillando la buena imagen de un verdadero estado de derecho.

Por otra parte, cabe mencionar que aún existen un sin número de delitos informáticos que no han sido tipificados adecuadamente y otros ni siquiera han sido considerados por nuestro sistema judicial, sin embargo, han sido plenamente identificados por los profesionales de la ciberseguridad. Entre estas prácticas de alto riesgo están las siguientes: a) captación de datos de geolocalización indebida; b) escaneo de redes; c) grabación sin autorización; d) ciberacoso, e) extorsión cibernética; f) secuestro Informático; g) homicidio mediante herramientas electrónicas; h) la persona que inculpe a otro de un delito informático; i) destrucción de evidencia digital.

Existe la posibilidad que un Hacker sea un profesional de la ciberseguridad. Ahora, la utilización del término “Hacker”, ha sido un tema de controversia a nivel mundial, debido a la dificultad de identificarlo como delincuente o experto en el área de la Seguridad Informática. En lo que respecta a Ecuador, luego del análisis realizado a las tipificaciones de los delitos informáticos que establece el

COIP, se puede decir que, el término Hacker, aunque no se encuentra de manera expresa en el código como tal, lo catalogaría como delincuente, dando lugar a que su capacidad de investigar sobre temas de ciberseguridad, vivan en el anonimato por temor a represalias.

Es necesario aclarar que el país atraviesa por una densa nube gris que no permite identificar los delitos cibernéticos. Es decir, la falta de cifras exactas de reportes de delitos informáticos, no implican la ausencia de los mismos; todo lo contrario, la incidencia de este tipo de actos criminales se encuentra latentes pero la identificación y denuncia de estos, no. Esto debido a que existen varios factores adicionales que lo impiden, entre los más comunes se tiene: el desconocimiento por parte de la víctima, la falta de capacidad investigativa por parte de los agentes del orden y el anonimato del atacante. El anonimato es un tema que un atacante experto ya conoce, para esto se vale de distintas herramientas y técnicas que eviten su identificación durante y después del cometimiento del ilícito, entre las herramientas más utilizadas por quienes desean mantener su anonimato está el uso de VPN que es una Red Privada Virtual, de esta manera una persona que se encuentra conectada en Ecuador puede aparentar estar situado en un país de cualquier otro continente.

Finalmente se menciona el caso emblemático que llamo la atención de la prensa nacional e internacional, y de mayor relevancia en este tipo de delitos en nuestro territorio denominado “caso OLA BINI”.

Siendo el principal sospechoso el ciudadano sueco, profesional de seguridad informática Ola Metodius Martin Bini , mismo que está siendo procesado por presunto ataque a la integridad de sistemas informáticos, de acuerdo a lo informado por la Fiscalía General del Estado en su BOLETÍN DE PRENSA **FGE N.º 066-DC-2019** en la ciudad de Quito, el 13 de abril de 2019 (FGE, 2019).

De acuerdo al criterio de los autores de este trabajo, el desconocimiento de lo que técnicamente implica un ataque a la integridad de sistemas, llevaría a las autoridades a cometer ciertos errores que no deben ser aceptables, esto implica que no se cumpla con el debido proceso. En este caso en

particular se conoce que al inicio se mencionó que se lo encontró en delito flagrante, lo cual debió ser demostrado dentro de las 24 horas subsiguientes por parte de la fiscalía en la audiencia de calificación de flagrancia como lo determina el Art. 529 del COIP, cabe aclarar que el Art. 532 fija que ninguna detención puede exceder más de 24 horas, pero la detención del Sr Ola Metodius Martin Bini duró 72 días y sin una acusación formal por parte de la Fiscalía. Se puede hablar de posibles errores sin intención, cercos mediáticos o simplemente una guerra legal en contra del acusado, pero a criterio de los investigadores se puede decir que evidentemente existe una falta de experticia en materia de delitos informáticos por parte de las entidades impartidoras de justicia y gubernamentales, si bien es cierto, no podemos mencionar todas las anoramalidades que incumplen con en el debido proceso, cualquier ciudadano puede sacar su propio criterio y conclusiones, observando el proceso No 17282-2019-01265 que se encuentra en la página del eSATJE .

CONCLUSIONES.

Se ha identificado los desafíos atraviesa la ciberseguridad ante la carente claridad de las leyes ecuatorianas en materia de delitos informáticos, tanto el desconocimiento de los juristas y autoridades han aportado a que los ciberdelincuentes se aprovechen de estas vulnerabilidades en el sistema judicial.

La correcta identificación de delitos informáticos ayudaría al jurista y autoridades competentes a no necesitar de realizar maniobras arriesgadas que falten al debido proceso para penalizar una conducta delictiva con el uso de medios electrónicos y desencadenados en el ciberespacio.

Se han identificado los delitos informáticos sin tipificar en nuestro Código y que el ciberdelincuente lo utiliza como vacío legal, con la finalidad de impulsar a futuro la debida regulación de leyes o dejar abierta la posibilidad a una reforma de las mismas. A pesar de esto, es menester aclar que la penalización nos ayuda a identificar y castigar un delito, pero es más que necesario que el país cuente con estrategias que prevengan el cometimiento de estos actos delictivos.

REFERENCIAS BIBLIOGRÁFICAS.

1. Arroyo 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.

2. Beiling, E. V. (1944). Esquema de Derecho Penal. Buenos Aires: Depalma.

3. Broy de la Cruz, H. (2013). HACKING & CRACKING. Lima: Macro EIRL.

4. Carrara, F. (1971). Programa de derecho Criminal. Parte general. Bogotá: Temis.

5. Asamblea Nacional del Ecuador. (2014). COIP. R.O.S 180. Código Orgánico Integral Penal. Quito: Finder Nacional.

6. El Comercio. (16 de 04 de 2019). 'Hackers' lanzaron ofensiva global para atacar web estatales. Quito - Ecuador.

7. El Comercio. (15 de 04 de 2019b). Al Ministerio del Interior le preocupa la legislación, tecnología y personal para enfrentar ciberataques en Ecuador. Quito; Nacional

8. Expreso. Ec. (2019). Las nueve razones del retiro del asilo a Assange, según el canciller Valencia. Redacción Expreso, 11 abril 2019. Ecuador

9. FGE, D. d. (13 de abril de 2019). Ciudadano sueco fue procesado por presunto ataque a la integridad de sistemas informáticos. Ciudadano sueco fue procesado por presunto ataque a la integridad de sistemas informáticos. Boletín de Prensa FGE Nº 066-Dc-2019. Fiscalía General Del Estado. Obtenido de https://www.fiscalia.gob.ec/ciudadano-sueco-fue-procesado-por-presunto-ataque-a-la-integridad-de-sistemas-informaticos/

10. Himanen, P. (2002). La ética del hacker y el espíritu de la era de la información. Elis.

11. ISO/IEC. (2012). Information Technology Security Techniques Guidelelines for cybersecurity. Geneva: ISO/IEC.

12. JTF, J. T. (2017). ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. Obtenido de Cybersecurity Curricular Guidelines | CSEC 2017: http://cybered.acm.org/

13. Larrieu-Let, CISM, E. (2015). Ciberataques ¿Estamos preparados? Buenos Aires: ISACA.

14. McAfee. (2018). The Economic Impact of Cybercrime-No Slowing Down. Santa Clara: McAfee.

15. RAE. (28 de agosto de 2019). Diccionario de la lengua española. Real Academia de Lengua Española. Obtenido de https://dle.rae.es

16. Ríos, R. H. (2003). La conspiración hacker. Buenos Aires: Longseller.

17. Rodríguez Canfranc, P. (2019). Ciberseguridad: Protegiendo la información vulnerable. Madrid: Fundación Telefónica.

18. Steven Raymond, E. (2001). Cómo convertirse en hacker. Biblioweb.

DATOS DE LOS AUTORES.

1. **Frankz Alberto Carrera Calderón.** Magister en Ingeniería y Sistemas de Computación. Docente de la Carrera de Derecho. Universidad Regional Autónoma de los Andes, Uniandes, Matriz Ambato – Ecuador. E-mail: ua.frankzcarrera@uniandes.edu.ec
2. **Joel Estuardo Quilligana Barraquel.** Ingeniero en Sistemas e Informática. Docente de la Universidad Internacional SEK Ecuador. E-mail: jequilligana.cib@uisek.edu.ec
3. **Mario Danilo Aguilar Martínez.** Magister en Derecho Penal y Criminología. Docente de la Carrera de Derecho. Universidad Regional Autónoma de los Andes, Uniandes, Matriz Ambato – Ecuador. E-mail: ua.marioaguilar@uniandes.edu.ec
4. **Santiago Fernando Fiallos Bonilla.** Magister en Derecho Económico Financiero y Bursátil. Docente de la Carrera de Derecho. Universidad Regional Autónoma de los Andes, Uniandes, Matriz Ambato – Ecuador. E-mail: ua.santiagofiallos@uniandes.edu.ec

RECIBIDO: 8 de noviembre del 2019. **APROBADO:** 19 de noviembre del 2019.