Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

Delitos informáticos en Ecuador según el COIP: un análisis documental

Computer crimes in Ecuador according to the COIP: documentary analysis

Crimes de computador no Equador de acordo com o COIP: uma análise documental

Viviana Vanessa Aparicio-Izurieta
viviana.aparicio@utelvt.edu.ec
https://orcid.org/0000-0002-1417-2036
Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador

RESUMEN

El presente articulo está enfocado a un análisis documental acerca de los delitos informáticos con mayores índices de frecuencia en el Ecuador y las sanciones establecidas en el COIP, mismo que es un compendio de reglas jurídicas de carácter penitenciario, o sea un compendio legislativo que instituye delitos y penas bajo el reglamento penitenciario ecuatoriano. Para el desarrollo de este trabajo se incluye una descripción teórica de cada uno de los delitos informáticos y las penalizaciones establecidas en el reglamento además de describir cuales son los fines más comunes al momento de realizar estos delitos y los mecanismos tecnológicos utilizados en los mismos. Para concluir se investiga que métodos o que propuestas tiene el estado nacional para asegurar la seguridad y confidencialidad de la información en cada una de las instituciones públicas o privadas, además de analizar si nuestro país cuenta con organismos especializados o leyes que logren dar una debida defensa a los múltiples sistemas informáticos y ciudadanos víctimas de estos delitos.

Palabras clave: Delitos, COIP, Penitenciario, Legislación.

ABSTRACT

This article is focused on a documentary analysis about computer crimes with the highest frequency rates in Ecuador and the sanctions established in the COIP, which is a compendium of legal rules of a penitentiary nature, that is, a legislative compendium that institutes crimes and penalties under Ecuadorian prison regulations. For the development of this work, a theoretical description of each of the computer crimes and the penalties established in the regulation is included, as well as describing what are the most common purposes at the time of carrying out these crimes and the technological mechanisms used in them. To conclude, it is investigated what methods or what proposals the national state has to ensure the security and confidentiality of information in each of the public or private institutions, in addition to analyzing whether our country has specialized agencies or laws that manage to give due defense. to the multiple computer systems and citizens who are victims of these crimes.

Keywords: Crimes, COIP, Penitentiary, Legislation.

RESUMO

Este artigo está focado em uma análise documental sobre os crimes de informática com as maiores taxas de frequência no Equador e as sanções estabelecidas no COIP, que é um compêndio de normas jurídicas de natureza penitenciária, ou seja, um compêndio legislativo que institui crimes e penas sob Regulamentos penitenciários equatorianos. Para o desenvolvimento deste trabalho, inclui-se uma descrição teórica de cada um dos crimes informáticos e das penas previstas no regulamento, bem como descrever quais são as finalidades mais comuns no momento da realização desses crimes e os mecanismos tecnológicos utilizados na eles. Para concluir, investiga-se quais métodos ou quais propostas o Estado nacional tem para garantir a segurança e confidencialidade das informações em cada uma das instituições públicas ou privadas, além de analisar se nosso país possui órgãos especializados ou leis que conseguem dar a devida defesa . aos múltiplos sistemas informáticos e aos cidadãos que são vítimas destes crimes.

Palavras-chave: Crimes, COIP, Penitenciária, Legislação.

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

Introducción

Gracias al gran desarrollo que ha tenido la tecnología informática se han revolucionado estilos de vida, formas de trabajar y la visión general de muchas cosas involucradas en el desarrollo social y económico de los países, es de esta forma que han surgido una serie de comportamientos ilícitos llamados, de forma genérica, delitos informáticos y de telecomunicaciones.

Las telecomunicaciones conforman uno de los sectores de más grande desarrollo tecnológico en el planeta. Las novedosas tecnologías brindan grandes ventajas para las comunidades, pero también pueden ser medios para que diversas personas tengan la posibilidad de hacer diferentes tipos de fraudes, mismos que afectan a usuarios, operadores de telecomunicaciones y proveedores de servicios a nivel general, ocasionando valiosas pérdidas no solo económicas sino también humanas.

Uno de los medios más utilizados para realizar estos tipos de delitos es la internet ya que permite la conectividad e interacción de muchas personas a nivel global, así como las facilidades para que la persona que ejecuta la infracción pueda ocultarse bajo una pantalla y cometer sus actos sin ser reconocido, buscado y en algunos casos sin ser quien indica ser, pasando a ser un delito muchas veces sin delincuente físico y sin evidencia que lo pruebe. Esta es la razón por la que estos tipos de delitos son difíciles de demostrar y muchas personas que son víctimas de los mismos prefieren no denunciar y solo resignarse a la pena de saber que fueron blancos de estos delincuentes.

Analizando estos factores se plantea este trabajo de investigación que busca orientar en cuanto a estos delitos informáticos y brindar una visión más generalizada sobre las medios y las formas que diversos bandidos manejan para realizar los mismos, además de analizar las penas establecidas en el COIP para cada caso de delito cometido, de esta forma se puede brindar a la ciudadanía la posibilidad de evitar sufrir estos delitos y en caso de hacerlo que sepan cómo actuar y qué medidas tomar para que no queden en la impunidad sus casos.

Para alcanzar el objetivo planteado se hará uso de varios métodos de investigación tradicional, como son el análisis y recopilado de información y su respectiva relación con los contextos actuales, brindando conceptos claros y claves como las medidas de seguridad informática a emplearse y haciendo ver los riesgos a los que se está expuesto dentro de la internet.

Metodología

Esta investigación está encaminada al estudio de los delitos informáticos más frecuentes en Ecuador, es decir, delitos que están logrando grandes alcances no solo económicos, sino que están repercutiendo gravemente en el correcto desarrollo del país de esta manera se determinó que la naturaleza para realizar esta investigación es de tipo cualitativa y comparativa ya que, mediante el uso de diversas fuentes de información brindaremos sobre cómo operan los delincuentes al momento de cometer estos delitos, los medios que utilizan y la frecuencia con que operan.

Esta investigación involucra un proceso de descripción narrativa proporcionado por la información compilada a través del cotejo de criterios. Además, planteamos que la investigación es analítica porque se realiza un análisis correspondiente de cada delito de lo establecido en el COIP y de su impacto a nivel nacional.

Desarrollo

Sabemos que en la actualidad nuestro país está en vías de desarrollo incluido los aspectos relacionados con la tecnología y con esto se da paso además a la evolución de las telecomunicaciones

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

conjuntamente con la enorme herramienta que se tiene en la actualidad y que permite la mayor parte de estos avances el llamado Internet; con lo cual se dan grandes ventajas pero de igual forma para cada beneficio se produce un peligro, en este caso son los delitos informáticos surgiendo así la necesidad de indagar sobre los delitos que se otorgan en Ecuador, ya que en algunas al ser delitos con poca evidencia física es muy difícil juzgarlos llegando a quedar muchos en la impunidad.

"Los delitos informáticos son actividades ilícitas realizadas por medios, tecnología y equipos de comunicación, con el objetivo de causar daños, desgastes o paralizar el uso de los sistemas informáticos." (Ramirez, 2017,p.1). Analizando esta definicion podriampos decir entonces que los delitos informaticos al igual que cualquier otro tipo de delito buscan un beneficio para quien los comete y causan una perdida para quien los sufre, partiendo de esto entonces al haber una relacion causa efecto deberian haber sanciones que pongan en la balanza estos dos factores y determinen una igualdad entre victima y victimario.

En el caso ecuatoriano, Zambrano-Mendieta, Dueñas-Zambrano y Macías-Ordóñez (2016) demostraron que en el regimiento jurídico nacional, se consagra el derecho a la protección de datos de carácter personal, a la intimidad personal, al derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, el delito informático atenta contra estos derechos específicos. Además, por la naturaleza de los delitos y la inexistencia de una legislación global alineada entre los países, existen dificultades para combatir los delitos informáticos (Campos, 2019), siendo aún más complejo este problema cuando se piensa en términos de cyber-espionaje, una estrategia usada por algunos países en la disputa gepolítica internacional (Waldman, Téllez & Sánchez, 2021). Asimismo, González-Sánchez et al (2019) argumentan que el Estado ecuatoriano debe priorizar la formación de recursos humanos y tecnologías adecuadas para implementar políticas públicas de combate a los crímenes informáticos lo que también demandará un sistema de monitoriamento y evaluación constante de estas políticas para que puedan ser eficientes (Ramos-Torres, Vieira, Jacobovski, 2021).

Estos delitos al no requerir de esfuerzos fisicos sino mas bien cualidades intelectuales se podria decir que cualquier persona puede transformarse en creador de un delito informático, a partir de un cliente, hasta terroristas u empresas criminales. Los que practican la delincuencia informática usualmente lo efectúan por medio de perfiles falsos, vínculos contenedores de virus informáticos, e-commerces falsas, páginas web fraudulentas, etc. Lo cual dificulta, en muchas situaciones, la identificación de dichos ciberdelincuentes.

Así como cualquier persona puede ser un delincuente informático también muchas situaciones que nos ocurren en la vida son un delito informático, pero a veces como no tenemos claro ciertos conceptos no podemos identificarlos aquí plantearemos una definición para los delitos informáticos más comunes según (Sanchis, 2021).

Fraude informático: en las estafas informáticas, los ciberdelincuentes buscan eliminar archivos, robar información personal, dinero, etc. Utilice métodos electrónicos. Esta acción intencionada puede afectar o eliminar el sistema operativo y el servidor.

Ciberacoso: este agravio hace referencia al develamiento de información interna o inclusive falsa y las amenazas tienen la posibilidad de llegar a hacer mucho mal a el individuo que lo sufre. En el ciberacoso se realizan uso de los medios digitales para acosar a una persona o conjuntos de individuos comúnmente de forma anónima y a lo largo de un lapso extenso de tiempo.

Transgresiones a la Propiedad Intelectual: Los delitos realizados contra la propiedad intelectual se manifiestan como robo o piratería y en algunos casos falseamiento, que son los delitos más frecuentes. Éstos trabajan contra una marca comercial realizando uso de copias de sus productos sin autorización previa de los autores de dichas marcas.

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

Sabotajes informáticos: Con sabotajes informáticos hacemos referencia a los delitos que tienen como fin remover, perjudicar, o cambiar funcionalidades de un sistema informático sin la previa autorización con el sencillo fin de obstaculizar su uso y su correcto funcionamiento.

Explotación infantil: este delito es uno de los más graves y se lo conoce como pornografía infantil, incluye a todo menor de edad es decir persona menor de 18 años que sea fotografiado o grabado mientras están siendo víctimas de abusos sexual o simplemente no lo saben, no lo hacen con su consentimiento, la distribución de dicho contenido no es legal por eso este contenido se ubica en la fracción más sombría de Internet. (p.1-2).

Ahora que sabemos cuáles son los delitos informáticos y como se materializan los mismos debemos conocer los medios que utilizan los delincuentes para cometer los mimos, como hablamos de delitos informáticos deducimos que en su mayoría se debe hacer uso de la tecnología, pero hay varios factores más que analizaremos.

“La ingeniería social es una colección de métodos que utilizan los cibercriminales para mentirle a los usuarios incautos para que les envíen datos confidenciales, infecten sus PCS con malware o abran enlaces a sitios infectados” (kaspersky, 2021, p.1). Este es uno de los mayores medios utilizados por delincuentes para comer delitos informaticos, como podemos analizar pueden utilizar tecnicas de observacion de sus victimas, sus rutinas, conocer mas su vida personal y de esta manera atacar.

Los Correos electrónicos son otro de los medios más manejados para ejecutar delitos informáticos, ya que la mayor parte de la población hace uso de estos en su trabajo, estudio o simplemente para su desarrollo personal, los delincuentes aprovechan esto para enviar correos haciéndose pasar por otras personas, buscando la confianza en sus víctimas para que estas accedan a abrir enlaces, o enviar información confidencial con la que luego actúan los atacantes.

Uno de los medios más famosos, efectivos y utilizado para cometer delitos informáticos son las redes sociales usadas en muchos casos para realizar lo que ya describimos como la famosa ingeniería social, la mayor parte de los internautas que hacen uso de las redes sociales publican en esta gran información de sus vidas personales como fotografías, ubicación, sitios de trabajo, sueldo de trabajo, lugar donde estudian, etc. Información que los delincuentes utilizan para estudiar a sus posibles víctimas y saber de este modo por donde atacar.

Las Páginas web son otro de los medios que utilizan los delincuentes informáticos para realizar sus acciones ilícitas, pueden actuar de varias formas, creando paginas falsas en donde piden cierto tipo de información personal a los usuarios y hasta suplantando paginas legales y frecuentemente visitadas, todo esto con el único fin de obtener de una u otra forma datos confidenciales para su posterior uso. Es necesario conocer a profundidad los medios y las formas en que estos delincuentes operan ya que es una de las formas de prevenir ser víctimas de estos ataques y alertar a familiares y conocidos, mientras más crece la tecnología más debe crecer nuestra necesidad de conocer lo bueno y lo malo que rodea estos avances sobre todo cuando somos nosotros los que hacemos uso de los mismos.

Pero ante tantos delitos y formas comunes de realizar los mismos que leyes nos resguardan, que dicen las autoridades y que medias son las legalmente establecidas para castigar estas acciones, vamos a hablar de ello a continuación.

Actualmente, el Ecuador cuenta con Leyes que condenan esta clase de delitos con penas de privación de libertad, los mismos que permanecen identificados en el (COIP).

Estos delitos son:

- Pornografía infantil – 13 a 16 años de privación de libertad
- Violación del derecho a la intimidad – de 1 a 3 años

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

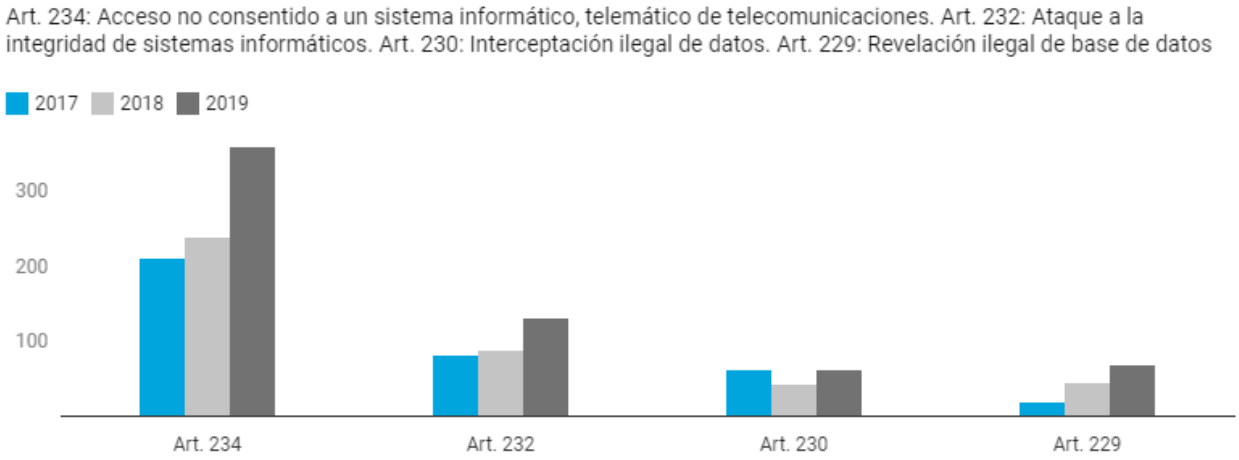
https://doi.org/10.51798/sijis.v3i1.284

- Develamiento ilegal de información de bases de datos – de 1 a 3 años de pena
- Interceptación de comunicaciones – de 3 a 5 años
- Pharming y Phishing – de 3 a 5 años
- Chantaje informático – de 3 a 5 años
- Ataque a la totalidad de sistemas informáticos – de 3 a 5 años de prisión
- Delitos contra la información pública reservada legalmente – de 3 a 5 años
- Ingreso no permitido a un sistema informático, telemático o de telecomunicaciones – de 3 a 5 años.

Como podemos analizar varios son los delitos que se encuentran tipificados dentro del COIP, pero la aplicación de los mismos se basa en ciertos criterios e interpretaciones.

Análisis y discusión de resultados

Analizando los tipos de delitos establecidos y en el COIP y existentes en nuestro país vemos que es la realización de los mismos es más usual de lo que podríamos pensar, solo en el intervalo del año 2021 se han denunciado 606 casos donde se apropian de manera ilegal de información y recursos por medios electrónicos en la Fiscalía General del Estado. En el 2020 se reconocieron 682 denuncias y en el 2019 fueron 828 denuncias, es decir que las estadísticas van en aumento.



Fuente: Fiscalía General del Estado.

En el transcurso del año 2021 en Ecuador se ha apresado a 3 bandas. Son en general 8 personas detenidas por delitos cibernéticos. Los delitos cometidos por esta banda van desde la apropiación de bienes de manera fraudulenta, hasta la pornografía infantil.

¿Qué debemos hacer entonces los ecuatorianos para evitar caer en la estrategia de la ingeniería social y de los otros muchos delitos informáticos?, es una pregunta que todos deberíamos empezar a realizarnos porque nadie está exento se ser víctima de estos hechos y de ser así es indispensable conocer como actuar para que los casos tengan justicia.

La Policía Nacional del Ecuador, expone varias sugerencias para eludir ser víctima de delitos informáticos.

- Evitar subir información personal en páginas web con origen desconocido o redes sociales.

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

- No acepte ofertas que estén a costos bastante bajos al mercar cualquier servicio sin cerciorarse de su credibilidad.
- Establezca contraseñas seguras.
- No comparta con otras personas sus contraseñas.
- No guarde contraseñas en computadores públicos para eludir las estafas.
- Verifique cuentas bancarias en computadores ajenas a su propiedad.
- Instale un buen sistema antivirus.
- No elimine los mensajes, correos electrónicos y toda información sospechosa, ya que estas van a servir en caso de que sea primordial denunciar frente a las autoridades.
- No fiar en correos electrónicos desconocidos.
- Vigilar a los menores cada que están conectados a la red

Son los varios los puntos a debatir en esta investigación sobre todo las sanciones establecidas en el COIP, algunos se preguntan y serán las más justas y en qué casos de aplican y en qué casos no. Que pasa cuando he sido víctima de delitos informáticos, pero no tengo pruebas físicas que así lo demuestren, tengo alguna posibilidad o simplemente estos casos quedan en el olvido, estas son algunas de las muchas interrogantes que cientos de personas se hacen.

"Un informe pericial es la prueba más eficaz para solucionar casos de procedencia informático" (escuelafintech, 2017, p.1). Es decir, hay expertos que se encargan de recolectar, analizar y resguardar las evidencias digitales para posteriormente emitir un informe donde se establecen las conclusiones finales de la investigacion, mismas que seran las utilizadas en los juicios y queb determinaran en gran medida la resoluasion del juez.

Sobre las sentiancias establecias en el COIP se sabe que "El fin primario de las penalidades, acorde al COIP, es la prevención general para la comisión de delitos; o sea, se amenaza castigar ciertas conductas con el objetivo de evadir su ejecución" (El Comercio, 2014, p.1). Sera esta una de las razones por la que algunas personas manifiestan que las sanciones son muy cortas, es un punto a analizar desde nuestra perspectiva.

Sera el transcurso de los años los que juzgaran el verdadero efecto del nuevo régimen en la sociedad ecuatoriana y en qué medida se cumple de manera efectiva las sanciones ante acciones ilícitas, y que beneficios nacionales se obtienen con las mismas.

Conclusiones

Sintetizando la información comparada y analizada durante este estudio, se puede evidenciar que las metas planteadas fueron concretadas, por medio de la aplicación de técnicas de recogida de datos y estudio de los mismos se planteó la información elemental para la identificación de los delitos informáticos más comunes y sus medios de realización para evitar de cierta forma ser víctimas de estos hechos.

El aumento de estos delitos informáticos se debe en gran medida a los progresos que está habiendo en cuanto a tecnología y a la poca información de los usuarios al hacer uso de los mimos, por ello es de vital importancia investigar sobre estos temas de interés nacional para tomar nuestras medias preventivas.

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.284

Hay que implementar todas las medias establecidas en las leyes ecuatorianas y las mencionadas anteriormente ya que estas son de vital importancia para evitar ser víctimas de estos casos y sobre todo para proteger nuestra información, debemos ser conscientes que nadie se entera de lo que no decimos o mostramos así que está en cada uno de nosotros cuidar nuestros datos ya que son uno de los bienes más importantes con lo que contamos y que dicen mucho de nuestro estilo de vida y de nuestra identidad.

REFERENCIAS

Campos, N. J. O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111.

El comercio. (17 de 08 de 2014). *elcomercio.com.* Obtenido de elcomercio.com: https://www.elcomercio.com/opinion/opinion-coip-derecho-penal.html

Escuelafintech. (17 de 12 de 2017). *escuelafintech.com.* Obtenido de escuelafintech.com: https://escuelafintech.com/que-es-perito-informatico/

Gonzáles, J., Hidalgo, C., Arce, J., & Ordoñes, P. (2019). Análisis y revisión sobre delitos informáticos en el Ecuador. In *Conference Proceedings UTMACH* (Vol. 3, No. 1, pp. 194-205).

Kaspersky. (19 de 12 de 2021). *latam.kaspersky.com.* Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Ramirez, R. (06 de 25 de 2017). *policia.gob.ec.* Obtenido de policia.gob.ec: https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Ramos-Torres C.A., Vieira, D. F., & Jacobovski, R. (2021). Estrutura institucional na avaliação e monitoramento de políticas públicas: uma análise nos países do MERCOSUL. Revista Brasileira de Administração Científica, 12(2), 232–245. https://doi.org/10.6008/cbpc2179-684x.2021.002.0019

Sanchis, E. (18 de 08 de 2021). *peritos-informaticos.com.* Obtenido de peritos-informaticos.com: https://peritos-informaticos.com/que-es-un-delito-informatico-y-que-tipos-existen

Waldman, D. H. G., Téllez, G. D. O., & Sánchez, P. G. S. (2021). El ciber-espionaje como herramienta estratégica de los actores internacionales en la era digital: una revisión desde la literatura. *Sapienza: International Journal of Interdisciplinary Studies*, *2*(4), 136-153.

Zambrano, K. I. D., & Ordoñez, L. M. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las ciencias*, *2*(2), 204-215.