DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR

Aura Dolores Zambrano Rendón
Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”
azambrano@espam.edu.ec. Calceta, Ecuador

Fausto Daniel Loor Campúes
Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”
fausto.loor@espam.edu.ec.edu.ec. Calceta, Ecuador

Wilmer Orley Zambrano Vera
Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”
wilmer.zambrano@espam.edu.ec. Calceta, Ecuador

Ramon Geovanny Párraga Vera
Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”
ramon.parraga@espam.edu.ec. Calceta, Ecuador

RESUMEN

El objetivo de la presente investigación es realizar una revisión bibliográfica sobre los delitos informáticos en tiempos de pandemia. Para ello se empleó la metodología bibliográfica, para indagar en diferentes fuentes los incidentes acontecidos y los tipos de ingeniería social usados para estos actos. 1. Búsqueda de información, se realizó en los exploradores Springer, Science Direct y Google Scholar, utilizando diferentes descriptores. 2. Selección y organización de los documentos electrónicos, se escogieron los documentos relacionados con los diferentes tipos de delitos informáticos en tiempos de pandemia. Y finalmente se realizó la revisión y análisis de la documentación que permitió determinar el número de personas afectadas con un total de 5048 esto sólo los casos denunciados, con un 43% suplantación de identidad, seguidos de la falsificación y uso de documentos falso.

Palabras claves: suplantación de identidad, COVID-19, ciberdelincuencia, ingeniería social.

ABSTRACT

The theft of personal data occurs when downloading software or performing any action with a service provider or others, is requested to give personal information to an entity or individual and this is done with it also occurs this type of act when this data is accessed through cyber-attacks, the latter being the one that causes greater havoc in society. Incidents that far from being reduced, have an increasing growth, especially in the COVID-19 pandemic, these figures have shot up exponentially. The purpose of this research is to carry out a detailed study of the crimes related to the subject to be treated, during the period of health emergency in Ecuador. To this end, a bibliographic methodology was used to investigate the incidents that occurred and the mechanisms used for these acts in different sources.

Keywords: Personal information, COVID-19, cyber-attack, hacking.

1. INTRODUCCIÓN

La pandemia del COVID-19 además de sus estragos sanitarios, también ha tenido un impacto negativo en el contexto de ciberseguridad a nivel mundial, donde han surgido diversas modalidades de Cibercriminalidad, Núñez & Carhuancho (2020) afirman que la ciberdelincuencia evolucionará conforme aumenta la cantidad de usuarios, lo que significa que también aumenta la cantidad y modalidad de ciberdelincuencia, y el Ecuador no ha sido la excepción a esta problemática, en donde los delitos informáticos se han incrementado durante la emergencia sanitaria, así como los diferentes tipos de delitos, entre ellos los de sustracción de datos personales que es la que atañe a esta investigación (Ajila, 2020).

Dada la situación sanitaria han surgido nuevas formas de conectarnos como sociedad a través de aplicaciones de internet, como las redes sociales, correo electrónico en dispositivos móviles, de escritorio y ahora las video llamadas usadas para la mayoría de nuestras actividades cotidianas, a causa de esto se ha llevado a que no solo se utilicen para actividades necesarias sino también delictivas sujetas a infracciones y sanciones (Vaca, 2016; Velásquez, 2019).

Según lo argumenta Peralta & Aguilar (2021) en el Ecuador tienen acceso al internet un 43 % de la población permitiendo estar conectados a la información que está en el ciberespacio lo cual es una puerta de entrada para los delincuentes, aumentando así el riesgo a la seguridad. Hasta hace poco en el Ecuador no había regulaciones ni limitaciones para el uso de los datos de los ciudadanos, aunque la constitución establece la protección de datos personales como un derecho las empresas públicas y privadas pueden hacer lo que sea con estos datos, por ejemplo pueden ser usados para crear publicidad para una segmentación del mercado, no obstante se convierte en un delito cuando se usa para manipular la intención de votos de los ciudadanos, según Primicias (2019) en Perú y Colombia existe una normativa vigente que protege y regule el uso de los datos por parte de las empresas y organismos nacionales e internacionales mientras que en el Ecuador aún estaba en proyecto hasta el 11 de mayo del 2021 cuando la asamblea dio por aprobada la Ley de protección de Datos Personales la cual se encargará de regular el flujo de datos digitalizados de los ecuatorianos (Imbaquingo, 2021; Dávalos, 2020).

Este marco legal de protección de datos personales, en otros países han surgido como un medio para salvaguardar el derecho a la privacidad de los ciudadanos en una época de creciente expansión de la tecnología, sus puntos claves son: conceptualizar a los datos personales; establecer la autoría y responsabilidad del manejo de datos; regular los aspectos básicos del tratamiento de datos, tales como la, el acceso, conservación, la seguridad, la confidencialidad (Cedeño, 2019); y determinar el grado de seguridad más apropiada para la transferencia de datos personales a otros países.

De acuerdo a las denuncias realizadas en las Fiscalías del Ecuador a nivel nacional, desde años anteriores a la actual pandemia del COVID-19, en el país se registraron 8421 casos de ciberdelincuencia en el 2017; estas cifras se incrementaron en 2018 a 9571 y de 10 279 en 2019. Dándose a notar una constante tendencia que sigue en crecimiento (El Universo, 2020c).

Según estas cifras se puede decir que la pandemia provocada por el coronavirus no ha hecho más que agudizar todo lo expuesto y elevar a índices inimaginables el riesgo cibernético al que están sometidas las empresas. El teletrabajo, la creciente popularidad de Internet y el uso de servicios por medios digitales requieren una atención urgente por parte de la alta dirección de las autoridades u organizaciones para evitar el robo de sus recursos económicos e información sensible.

2. METODOLOGÍA

Para el desarrollo de este trabajo se utilizó la técnica de investigación documental con la finalidad de recopilar y seleccionar información sobre los diferentes delitos informáticos en el Ecuador a través de publicaciones de los principales diarios del país, artículos científicos y noticias; los cuales posibilitarán determinar el impacto que han tenido las diferentes técnicas de ingeniería social durante la pandemia COVID-19.

De acuerdo a la revista de investigación y desarrollo I+D, en su artículo Evolución de la COVID-19 en Ecuador (Parra & Carrera, 2020), los primeros casos se reportaron el 29 de febrero de 2020; es por eso que a partir de esta fecha se planteó

la búsqueda de información en diferentes motores de búsqueda entre las principales se tiene Springer, ScienceDirect y Google Scholar, utilizando los siguientes descriptores:

- Delitos informáticos
- COVID-19
- Ecuador
- Robo de información
- Sustracción de identidad
- Fraude informático
- Fiscalía general del estado

Una vez realizada la selección de los artículos y noticias de los diferentes periódicos, se efectuó una matriz donde se consideraron los criterios de título, tipo de ataque, autores, año y tipo de documento. Y finalmente realizar un análisis de los documentos seleccionados con la finalidad de conocer los diferentes tipos de delitos informáticos que se han cometido durante la pandemia COVID-19 y el porcentaje de usuarios afectados.

De acuerdo a la metodología expuesta se definieron las siguientes etapas para el proceso de recolección de información:

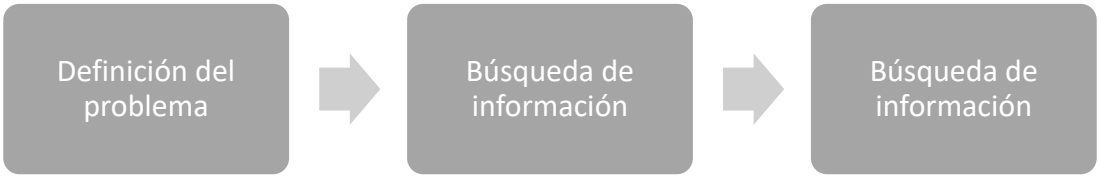

Fig. 1. Proceso para la recolección de información.
Fuente: elaboración propia

3. RESULTADOS Y DISCUSIÓN

Definición del Problema:

Toda vez que llegó la pandémica, la mayoría de las empresas públicas y privadas en el Ecuador y nivel Internacional se vieron en la necesidad llevar sus actividades de manera online, pero la gran mayoría de las empresas a nivel de América registraron importantes caídas de sus ingresos y presentan dificultades para mantener sus actividades por lo que tuvieron que cerrar.

Además, las escuelas, colegios y universidades también empezaron a trabajar de manera online, y consigo el uso de las TIC aumentaron, por lo que la mayoría de las actividades se realizan usando estas herramientas tecnológicas y consigo aumentó en un gran porcentaje de los procesos online como: compras, pagos, transacciones, negocios y ventas.

A nivel nacional se presenta un sin número de denuncias en la Fiscalía General del Estado (2020) por delitos informáticos de diferentes tipos. De acuerdo a los resultados obtenidos se dan a conocer que existen un total de 5048 denuncias desde enero hasta agosto del 2020 derivadas del delito informático acorde a los artículos 178, 186, 190, 229, 230, 231 y 232 del Código Orgánico Integral Penal COIP (conforme a la Tabla 1). Si la tendencia continua casi se igualará a los casos del 2019. Esto actualmente es un problema social que existe por el desconocimiento de las personas.

Selección y organización de los documentos electrónicos: Se realizó la búsqueda de información en distintas plataformas para obtener un buen porcentaje de publicaciones que sustenten la situación actual, también se indago en la web específicamente en Google para obtener artículos de sustento teórico y científicamente respaldado.

Tabla 1. Matriz resumen de documentos electrónicos seleccionados para análisis

Título	Tipo de ataque	Autor(es)	Año	Tipo de documento
Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios	ninguno	Acosta, María; Benavides, Merck; García, Nelson	2020	Artículo Científico
Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro	Suplantación de identidad	El Universo	2020	Informativo
Los robos cibernéticos encienden las alertas en Ecuador	Phishing	El Comercio	2020	Informativo
Cómo opera la ciberdelincuencia y por qué es difícil detectarla y sancionarla Sniffing wi-fi	Suplantación de identidad	El Universo	2020	Informativo
12 ataques por segundo se registran en Ecuador	Suplantación de identidad	El Telégrafo	2021	Informativo
Ciberataques: una pandemia maliciosa para la seguridad empresarial	Malware	Revista gestión	2020	Informativo
Ciberdelincuentes acechan tus datos en aplicaciones para video llamadas; seis tips para estar protegidos	Sniffing	El Universo	2020	Informativo
Ciberdelincuentes lanzan ataques informáticos con falsas foto multas de tránsito en Ecuador.	Phishing, Suplantación de identidad	El Comercio	2021	Informativo
Ciberdelitos aumentan durante la emergencia	Suplantación de identidad	El Telégrafo	2021	Informativo
Ciberdelitos en Ecuador crecen durante la pandemia	Extorsiones, robos, suplantación de identidad y acoso	NotiMundo Al Día	2020	Informativo
Ecuador, una de las naciones más atacadas por los 'hackers'	ransomware	El Comercio	2021	Informativo
Hackeos en cuentas bancarias, ¿qué hacer, ¿quién debe responder por el mismo y cómo evitarlo?	Malware, vishing	El Universo	2021	Informativo
Los ataques de fuerza bruta ponen en riesgo a los usuarios digitales	Fuerza bruta (diccionario)	El Comercio	2020	Informativo
Redes sociales son el nicho ideal para los ciberdelitos en Ecuador	Phishing	El Universo	2020	Informativo

Revisión y análisis de la documentación: Se realizó un análisis exhaustivo y detallado de los documentos seleccionados lo que permitió observar y conocer los diferentes tipos de ataques que son más influyentes durante la pandemia, además conocer cuáles son las herramientas tecnológicas que fueron utilizadas para el robo de información (conforme a la Tabla 1).

De acuerdo con el análisis de las revisiones bibliográficas, el tipo de ataque que más se ha utilizado para el robo de información (conforme a la Tabla 2) durante la pandemia es la suplantación de identidad representando esto un 43% de los 5048 casos de denuncias que se realizaron y que se verificaron según los procedimientos policiales.

Tabla 2. Delitos informáticos en Ecuador

DELITOS	CONSUMADOS
Suplantación de identidad	2162
Falsificación y uso de documento falso	1448
Apropiación fraudulenta por medios electrónicos	1033
Acceso no concedido a un sistema informático, telemático o de telecomunicaciones	175
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	85
Ataques a la integridad de sistemas informáticos	51
Intercepción ilegal de datos	45
Transferencia electrónica de activos patrimonial	31
Revelación ilegal de base de datos	18
Total de Delitos	5048

Fuente: fiscalía general del Estado (2020)

Las 3 principales formas que suponen un delito informático y que son las más usadas como modus operandi por los delincuentes cibernéticos, para ejecutar sus herramientas informáticas desarrolladas por ellos mismo o modificadas son la suplantación de identidad con 2162 casos reportados que representan un 43% del total de casos, falsificación y uso de documentos falsos con 1448 que representan un 29% del total de casos casi igualados con el 3er puesto que es la apropiación fraudulenta por medios electrónicos con 1033 que representan un 20% del total de casos, entre estas 3 formas suponen un 92% de todos los delitos reportados, lo que nos deja 405 casos de diferentes delitos informáticos que representan un 8% del total de casos los cuales se muestran el Tabla 3.

Tabla 3. Delitos informáticos en Ecuador

Delitos	Frecuencia Absoluta	Frecuencia Relativa
Suplantación de identidad	2162	42,83%
Falsificación y uso de documento falso	1448	28,68%
Apropiación fraudulenta por medios electrónicos	1033	20,46%
Acceso no concedido a un sistema informático, telemático o de telecomunicaciones	175	3,47%
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	85	1,68%
Ataques a la integridad de sistemas informáticos	51	1,01%
Intercepción ilegal de datos	45	0,89%
Transferencia electrónica de activos patrimonial	31	0,61%
Revelación ilegal de base de datos	18	0,36%
Total	**5048**	**100%**

4. DISCUSIÓN

En un estudio realizado por Bartolomé & Monteiro (2021) describen el rol del COVID-19 como conductor de inseguridad o potenciador de riesgo en el campo de la ciberseguridad. Se detallan algunos casos de ciberataques tales como el phishing, el robo de información personal de un individuo a través de un engaño, por lo general apelando a correos electrónicos o páginas web falsas. Algunos ejemplos de ciber-espionaje que alcanzaron notoriedad internacional incluyen el

ataque perpetrado contra el Bundeaste (Parlamento alemán) hace un lustro, cuando varios legisladores recibieron falsos correos electrónicos que implicaron la descarga involuntaria de un malware que posibilitó el robo de gran cantidad de información.

En el mismo indica que las técnicas de phishing fueron responsables de al menos el 90% de las infecciones por malware, así como del 72% de las filtraciones de datos en organizaciones. Durante el primer semestre de 2020 los ataques con phishing y malware pasaron de menos de 5.000 a más de 200.000 por semana. En ese lapso, la cantidad de ciberataques a nivel global creció un 34% respecto al período inmediato anterior.

En el caso de América Latina y el Caribe se verificó un fuerte aumento de casos de phishing y de campañas de estafas en relación con la COVID -19, que aprovechan la crisis del coronavirus y el consiguiente confinamiento. Así, los ataques con phishing que tenían software malicioso adjunto tuvieron en la región un aumento interanual del 17% en enero, 52% en febrero y 131% en marzo. En términos absolutos, los ciberataques con malware en América Latina y el Caribe habrían sido unos tres millones, aproximadamente, durante el primer trimestre del año.

Otro estudio bibliográfico realizado por Miró, 2021 titulado “Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos”. En el mismo se detallan varias fuentes de las principales empresas que se encargan del manejo de la ciberdelincuencia; primeramente, tenemos los informes de transparencia de Google que muestran, desde el 15 de marzo, tanto un incremento acelerado del número de sitios de suplantación de identidad existentes como de los detectados por semana. El informe sobre ciberseguridad durante los cien primeros días de la COVID-19 de MIMECAST23 muestra que la detección de spam tuvo un incremento del 26,3%, la detección de suplantación de identidad aumentó en 30,3%, la detección de malware un 35,16% y el bloqueo de clics por URL peligrosas se incrementó en un 55,8% en relación con la primera semana del año.

El primer estudio que ha tratado de analizar de forma general el impacto de la pandemia en el cibercrimen es el de Hawdon et al., (2020), quienes realizaron encuestas de cibervictimización para siete ciberdelitos en dos momentos diferentes, uno entre el 24 y el 30 de noviembre de 2019, y otro entre el 14 y el 17 de abril de 2020. Los autores no encontraron diferencias estadísticamente significativas para los siete delitos en conjunto y tan solo el delito de robo de datos mostró diferencias significativas, siendo el resultado el contrario al esperado, con una mayor tasa en el grupo «pre-COVID-19».

CONCLUSIONES

Como se puede evidenciar la sustracción de datos es muy común en la sociedad con el avance de la tecnología y más con la pandemia del COVID-19, donde se reflejó un incremento de los diferentes delitos informáticos, donde los ciberdelincuentes crearon estrategias más convincentes de ingeniería social.

Los casos que reposan en la fiscalía son 5048, sin analizar los casos que no han sido denunciado por los usuarios, algunos por desconocimiento y otros por temor a represalia de los ciberdelincuentes; es importante mencionar que en el código penal incorpora una serie de infracciones delictivas, que se encuentran tipificadas y sancionan de acuerdo a cada tipo penal.

REFERENCIAS

Acosta, M., Benavides, M., & García, N. (2019). Vista de Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89), 351-368. https://produccioncientificaluz.org/index.php/rvg/article/view/31534/32619

Ajila, A. (2020). Análisis jurídico de las leyes que amparan a víctimas del delito informático en Santo Domingo. Universidad Regional Autónoma De Los Andes.

Bartolomé, M., & Monteiro Lima, A. G. (2021). el ciberespacio, durante y después de la pandemia COVID-19. Revista de la Academia del Guerra del Ejército Ecuatoriano, 14(1), 10. https://doi.org/10.24133/age.n14.2021.06

Cedeño, I. (2019). Análisis de la seguridad de información en el área de secretaría de la Universidad Laica “Eloy Alfaro” de Manabí, Extensión El Carmen. Revista Científica de Informática ENCRIPTAR, 2(3), 10-11. https://publicacionescd.uleam.edu.ec/index.php/encriptar/article/view/90/
185

Dávalos, N. (2020, octubre 12). La Ley de Protección de Datos: un proyecto prioritario, aunque poco tratado. Primicias. https://www.primicias.ec/noticias/tecnologia/ley-proteccion-datos asamblea/

El Comercio. (2021a). Ecuador, una de las naciones más atacadas por los ‘hackers’. https://www.elcomercio.com/tendencias/ecuador-naciones atacadas-hackers-tecnologia.html

El Comercio. (2021b). Los ataques de fuerza bruta ponen en riesgo a los usuarios digitales | El Comercio. https://www.elcomercio.com/tendencias/hackers-ciberataques-fuerza bruta-usuarios.html

El Comercio. (2021c). Ciberdelincuentes lanzan ataques informáticos con falsas foto multas de tránsito en Ecuador | El Comercio. https://www.elcomercio.com/tendencias/ciberdelincuentes-ataques falsas-fotomultas-ecuador.html

El Telégrafo. (2021a). 12 ataques por segundo se registran en Ecuador. https://www.eltelegrafo.com.ec/noticias/judicial/12/delitosinformaticos-coip-policia-fiscalia

El Telégrafo. (2021b). Ciberdelitos aumentan durante la emergencia. https://www.eltelegrafo.com.ec/noticias/economia/4/ciberdelitos emergencia-sanitaria-ecuador

El Universo. (2021). Hackeos en cuentas bancarias, ¿qué hacer, ¿quién debe responder por el mismo y cómo evitarlo? https://www.eluniverso.com/larevista/tecnologia/hackeos-en-cuentas bancarias-que-hacer-quien-debe-responder-por-el-mismo-y-como evitarlo-nota/

El Universo. (2020a). Ciberdelincuentes acechan tus datos en aplicaciones para video llamadas; seis tips para estar protegidos. https://www.eluniverso.com/noticias/2020/09/28/nota/7994425/delitos informáticos-internet-casos-reales-redes-sociales-ecuador/

El Universo. (2020b). Cómo opera la ciberdelincuencia y por qué es difícil detectarla y sancionarla.
https://www.eluniverso.com/noticias/2020/09/27/nota/7991998/delitos informáticos-internet-casos-reales-redes-sociales-ecuador/

El Universo. (2020c). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos informáticos-internet-casos-reales-redes-sociales-ecuador/

El Universo. (2020d). Redes sociales son el nicho ideal para los ciberdelitos en Ecuador.
https://www.eluniverso.com/noticias/2020/09/27/nota/7991326/delitos informáticos-internet-casos-reales-redes-sociales-ecuador/

Fiscalía General del Estado. (2020). Fiscalía General del Estado | Cifras de robos. https://www.fiscalia.gob.ec/estadisticas-de-robos/

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. American Journal of Criminal Justice 2020 45:4, 45(4), 546-562. https://doi.org/10.1007/S12103-020-09534-4

Imbaquingo, J. (2021, mayo 12). Ley para la protección de datos de los ecuatorianos; se creará una Superin-tendencia. El Comercio. https://www.elcomercio.com/actualidad/politica/ley-proteccion-datos-ciudadanos-ecuador.html

Miró Llinares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. IDP. Revista de Internet Derecho y Política, 32, 1-17. https://doi.org/10.7238/idp.v0i32.373815

NotiMundo al Dia. (2020). Ciberdelitos en Ecuador crecen durante la pandemia. https://notimundo.com.ec/ciberdelitos-en-ecuador-crecen durante-la-pandemia/

Núñez Pérez, F. V., & Carhuancho Zaldaña, B. (2020, febrero 11). Ciberdelincuencia en tiempos de COVID-19: ¿La vulneración a derechos constitucionales? Lumen, 16(1), 93-100. https://doi.org/10.33539/lumen.2020.v16n1.2287

Parra, M., & Carrera, E. (2020). Evolución de la COVID-19 en Ecuador. Investigación & Desarrollo, 13(1), 28-42. https://doi.org/10.31243/ID.V13.2020.1002

Peralta Zuñiga, M. L., & Aguilar Valarezo, D. N. (2021, junio 8). Vista de La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad y Auditoría, 53, 99-126. https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061/2797

Primicias. (2019). Ecuador es uno de los tres países de la región donde falta una ley que proteja los datos personales. https://www.primicias.ec/noticias/tecnologia/ecuador-desprotegido-ley datos-personales/

Revista Gestión. (2020). Ciberataques: una pandemia maliciosa para la seguridad empresarial Gestión. https://www.revistagestion.ec/estrategia análisis/ciberataques-una-pandemia-maliciosa-para-la-seguridad empresarial

Rosero, A. (2020). Los robos cibernéticos encienden las alertas en Ecuador. https://www.elcomercio.com/actualidad/robos-ciberneticos-alertas ecuador-denuncias.html