UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE DELITOS INFORMÁTICOS RELEVANTES EN ORGANIZACIONES GUBERNAMENTALES EN AMÉRICA LATINA

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: BYRON JOEL TERÁN VILLAFUERTE

TUTOR: JOE LLERENA IZQUIERDO

Guayaquil – Ecuador

2022

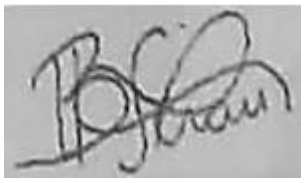
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Byron Joel Terán Villafuerte con documento de identificación N° 0931544910 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 15 de junio del año 2022

Atentamente,



_____

Byron Joel Terán Villafuerte
0931544910

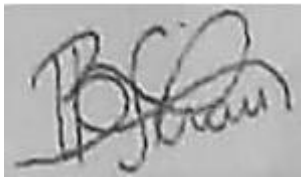
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Byron Joel Terán Villafuerte con documento de identificación No. 0931544910, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Nombre del artículo sin punto final", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 15 de junio del año 2022

Atentamente,



_____

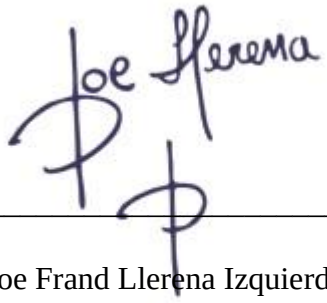
Byron Joel Terán Villafuerte
0931544910

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE DELITOS INFORMÁTICOS RELEVANTES EN ORGANIZACIONES GUBERNAMENTALES EN AMÉRICA LATINA, realizado por Byron Joel Terán Villafuerte con documento de identificación N° 0931544910, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 15 de junio del año 2022

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Este trabajo fruto de mi esfuerzo y dedicación se lo dedico primero a Dios por permitirme llegar a este momento tan especial en mi vida, a mis padres pilares fundamentales en mi vida que con su paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía. A mis profesores, gracias por su tiempo, por su apoyo, así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

Finalmente quiero dedicar esta tesis a todos los que estuvieron acompañándome en este proceso, por apoyarme, por extender su mano en momentos difíciles y por el amor brindado cada día.

AGRADECIMIENTO

Primeramente, doy gracias a Dios por permitirme cumplir una de mis metas, gracias a mis padres por ser los principales motores de mis sueños, gracias a mi familia por apoyarme en cada decisión y proyecto, gracias a mi universidad por ayudarme a convertirme en un profesional en algo que me apasiona, gracias a los maestros que fueron parte de este proceso de formación integral.

Este proyecto representa años de esfuerzo y dedicación por lo que jamás me alcanzarán las palabras para agradecer a cada persona que aportó a este gran logro que más que mío es de todos aquellos que lo hicieron posible y jamás me alcanzarán las palabras para agradecerles, por tanto.

RESUMEN

Los delitos informáticos tienen un considerable impacto en toda persona o empresa privada o empresa pública en cualquier país o sociedad. El objetivo general de este trabajo de investigación es analizar los delitos informáticos frecuentes direccionados a las instituciones gubernamentales para su clasificación mediante una revisión de literatura relevante. Se realiza una investigación analítica-descriptiva de enfoque cuantitativo. El alcance exploratorio en su fase inicial permite analizar la delincuencia informática en la literatura científica y relevante seleccionados de librerías digitales. Entre los resultados están, la identificación de literatura pertinente en el tema de delincuencia informática que afectan a las instituciones gubernamentales en Latinoamérica, la clasificación de los delitos informáticos que afectan a las instituciones gubernamentales en Latinoamérica, y el contraste de los resultados obtenidos para producir una matriz detallada de medidas preventivas en Ecuador. Se concluye que los gobiernos deben aplicar o crear políticas para prevención proactiva, reconocer los ataques que pueden ser objeto, adoptar herramientas tecnológicas para mitigar los delitos y especialización del talento humano de sus organizaciones dependientes.

Palabras claves: Ciberdelincuencia, piratas informáticos, organizaciones gubernamentales, Latinoamérica, ataques cibernéticos.

ABSTRACT

Computer crimes have a considerable impact on any person or private company or public enterprise in any country or society. The general objective of this research work is to analyze the frequent computer crimes directed to governmental institutions for their classification through a review of relevant literature. Analytical-descriptive research with a quantitative approach is carried out. The exploratory scope in its initial phase allows analyzing computer crime in scientific and relevant literature selected from digital libraries. Among the results are, the identification of relevant literature about computer crime affecting governmental institutions in Latin America, the classification of computer crimes affecting governmental institutions in Latin America, and the contrast of the results obtained to produce a detailed matrix of preventive measures in Ecuador. It is concluded that governments should apply or create policies for proactive prevention, recognize the attacks they may be subject to, adopt technological tools to mitigate crimes and specialize the human talent of their dependent organizations.

Key words: Cybercrime, hackers, government organizations, Latin America, cyber-attacks.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

El “cybercrime” o delito cibernético es una actividad delictiva realizada a través de una computadora para acceder, transmitir o manipular datos ilegales, también se denomina actividad ilícita en línea; esta actividad es contra de la ley (Pérez González, 2021)(Toala Indio, 2021), es una intrusión en un sistema informático o base de datos de un tercero, es un robo de datos almacenados o daño de equipos y datos (Moncayo Ronquillo, 2021)(de la Nube Toral Sarmiento et al., 2018)(Aguirre Sánchez, 2021). En esta época actual existe gran dependencia de Internet, y esto recae en varios tipos de delitos cibernéticos como: robo de identidad, pornografía, sustitución de correo electrónico, robo financiero, terrorismo cibernético, entre otros (Batra et al., 2020)(Ayala Carabajo et al., 2016)(Escalante Quimis, 2021).

Las personas sencillas tienen más habilidades de uso de Internet y existe un aumento en los delitos relacionados con la tecnología que comprometen la seguridad y privacidad; los gobiernos toman medidas posibles en el área de seguridad (Morán Maldonado, 2021); además otras organizaciones relacionadas se acogen a las medidas por daños a la reputación y acciones legales (Rosero Tejada, 2021). Para contrarrestar el “cybercrime” se crea la “cybersecurity” o seguridad cibernética que es una seguridad de Tecnología de la Información y contiene técnicas/modelos/arquitecturas para evitar el robo de datos o evitar la interrupción de los sistemas informáticos y hardware (Mallika et al., 2018)(Vera Navas, 2021).

De acuerdo a la agencia federal de investigación e inteligencia, FBI, de Estados Unidos en el año 2021 hay 847376 denuncias por delitos informáticos que representan 6.9 billones de dólares americanos a nivel mundial (FBI, 2021); se reportan arrestos en Estados Unidos y Londres, las victimas de fraudes se reportan desde Mundo occidental y Asia, Reino Unido, Estados Unidos, Australia, Canadá, Hong Kong, Malasia y Singapur (Hamisu et al., 2021).

Durante la emergencia del Covid-19 en el año 2020 por transmisión del virus, los delincuentes aprovecharon el encierro de las personas y los delitos informáticos aumentaron (Tacuri López, 2021)(Coello Ochoa, 2021), después de la pandemia estos delitos aumentaron cinco veces, además está en continuo aumento la cantidad de usuarios en Internet (Amarullah et al., 2021).

De acuerdo al Foro Económico Mundial, el cybercrime es una amenaza para las empresas y para la economía mundial, es decir están en riesgo las grandes de todo tamaño, los atacantes estudian las vulnerabilidades de los sistemas o redes (Terán Terranova, 2021)(Alvarado

Ronquillo, 2021)(Ayala Carabajo & Llerena Izquierdo, 2017); en Ecuador durante el 2018 se reportaron 817 denuncias por delito informático (Toapanta Toapanta et al., 2020). El COIP refiere a delitos informáticos en los Art. 173, 174, 186, 190, 229, 230 al 234 (Ron et al., 2018).

Los delincuentes seleccionan fuentes de datos o sistemas, los ataques son dirigidos a personas, empresas, infraestructuras nacionales, diversos sectores gubernamentales y gobiernos (Orozco Bonilla, 2021); los ciber delincuentes utilizan las tecnologías de Internet y causan un daño significativo (Miranda Jiménez, 2021); los efectos secundarios de los ataques son un riesgo para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional vinculada (Oni et al., 2019).

Los ciberataques generan un impacto negativo en la situación económica de un país, la defensa contra los delitos informáticos es una lucha para las personas y organizaciones, los ciber delincuentes conocen y utilizan técnicas más complejas, los delitos informáticos están en aumento debido a varios factores (Ponce Larreategui, 2021)(Holguín Mendoza, 2021), además existe una gran necesidad de ahondar en el análisis de los casos de esta clase de crimen y estar preparados (Batra et al., 2020)(Chévez Morán, 2021).

Existen amenazas a empresas individuales, comerciales y gubernamentales, además existen varios desafíos como mantener a la vista la seguridad del sistema empresarial, los diseñadores de seguridad han introducido múltiples perímetros como firewalls y detección y respuesta de amenazas (Yarali & Sahawneh, 2019)(Guaigua Bucheli, 2021).

Las personas temen sobre el peligro del delito informático, sin conocer sus detalles y esta razón es necesario la investigación para clasificarlos.

El objetivo general es analizar los delitos informáticos frecuentes direccionados a las instituciones gubernamentales de Latinoamérica para su clasificación mediante una revisión de literatura relevante.

Entre los resultados están: Identificación de literatura pertinente en el tema de delincuencia informática que afectan a las instituciones gubernamentales en Latinoamérica, Clasificación de los delitos informáticos que afectan a las instituciones gubernamentales en Latinoamérica, y Contrastar los resultados obtenidos para producir una matriz detallada de medidas preventivas en Ecuador.

Se concluye que los gobiernos deben aplicar o crear políticas para prevención proactiva, reconocer los ataques que pueden ser objeto, adoptar herramientas tecnológicas para mitigar los delitos y especialización del talento humano de sus organizaciones dependientes.

2. REVISIÓN DE LITERATURA

2.1. Una perspectiva del cybercrime

El cybercrime es una infracción realizada en un dispositivo técnico, como una computadora, un teléfono inteligente y conexión a Internet, hay dos tipos de delitos informáticos: el delito ciberdependiente que se ejecuta con TICs, y el delito cibernético que es un delito convencional con un alcance más amplio hecho posible por la TICs (Amarullah et al., 2021).

Se utiliza parte de una aplicación informática o una red y el delito es cualquier actividad, comportamiento o posesión ilegal que vulnere las reformas o los procedimientos legales; los delincuentes cibernéticos pueden ser programadores, distribuidores, expertos en TI, estafadores, cajeros, vendedores de correo negro o piratas informáticos (Sattar et al., 2019).

Es una actividad delictiva como vulneración electrónica hasta los ataques de denegación de servicio mediante el uso de una computadora o red informática como herramienta, además el ciberdelito es considerado un crimen transfronterizo y transnacional (Sandjojo et al., 2020).

2.2. Técnicas contra delitos informáticos

Algunos algoritmos o técnicas que se utilizan para detectar o prevenir los delitos informáticos son: Inteligencia Artificial, Clustering, Redes Neuronales, Reglas de Asociación, Árboles de Decisión, Regresión, Algoritmo Genético, minería de datos y el aprendizaje automático (Batra et al., 2020).

2.3. Tipos de delitos informáticos

El robo de identidad, Spoofing de correo electrónico, Robo financiero, Acecho cibernético, ciber pornografía, tráfico de drogas (Batra et al., 2020), piratería/hacking, agrietamiento, difamación, material obsceno, Spoofing, Phishing (Mallika et al., 2018), malware, DDOS, fraude (Amarullah et al., 2021), skimming de pagos en línea, Publicación o transferencia no autorizada de información personal, Piratería / virus / spam, desaparición a través de medios electrónicos, difusión de información falsa, acoso sexual, intimidación, distribución de pornografía infantil, Violación de sistemas para acceder u obtener protegido información (Ron

et al., 2018). Los tres tipos de delitos dominantes son: Compromiso de correo electrónico, Fraude de confianza / romance y Falta de pago / No entrega (Ahmed et al., 2019).

Manipulación con documentos de origen informático, hackear con sistema informático, recibir computadora o dispositivo de comunicación robado, uso de la contraseña de otra persona, engaño con el uso de recursos informáticos, publicación de imágenes privadas de otros, publicación información obscena en formato electrónico (Kapoor et al., 2020).

De acuerdo a las Naciones Unidas que verifica la ciberseguridad de los 193 países miembros, esta organización publica índices globales de ciberseguridad que se basan en: legal, técnico, organizacional, capacidad de construcción y cooperación; el índice combina 25 indicadores para monitorear la implementación de la ciberseguridad (Toapanta, Pesantes, et al., 2020).

Existen vulnerabilidades que los delincuentes aprovechan como: Falta de programas contra amenazas a la ciberseguridad, desconocimiento del impacto potencial de los ataques cibernéticos, descuido de los empleados en el manejo de información y datos, los controles de seguridad de la información están obsoletos, dificultad para identificar datos sospechosos en la red (Toapanta, Ochoa, et al., 2019).

3. METODOLOGÍA

Se realiza una investigación analítica-descriptiva de enfoque cuantitativo; el alcance exploratorio en su fase inicial permite analizar la delincuencia informática en la literatura científica y relevante seleccionada de librerías digitales. La técnica de la observación para verificación de los artículos e informes sobre delincuencia informática y la Universidad Politécnica Salesiana proporciona acceso a estas bibliotecas digitales.

Se utiliza la revisión sistemática de literatura (De Oliveira et al., 2021) que especifica el procedimiento para localizar documentos, seleccionar, valorar contribuciones, realizar un análisis y sumario de datos, todo es un estudio preliminar sobre delincuencia informática para responder a la pregunta: ¿Cuáles son delitos informáticos direccionados a las instituciones gubernamentales?. Se siguen 5 pasos que se presentan en la Fig. 1.

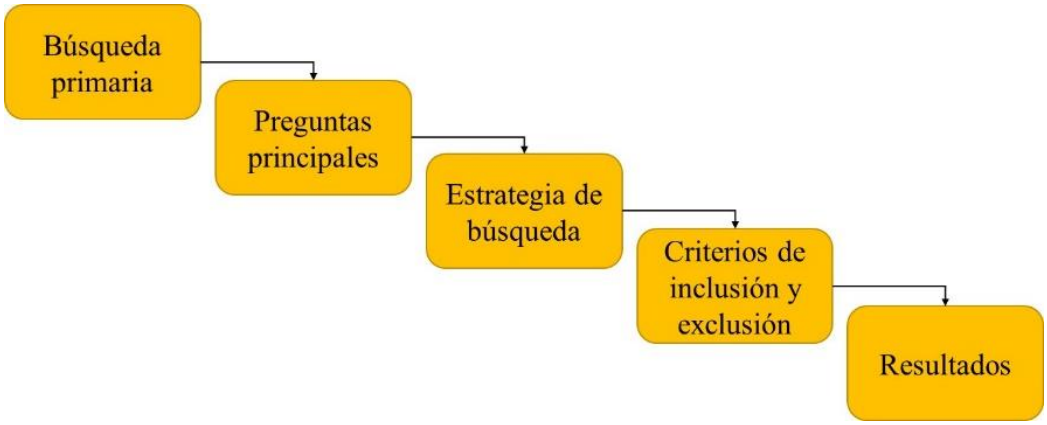


Figura 1. Revisión sistemática de la literatura

Búsqueda principal: Dirigir el estudio preliminar al área: a) cybercrime government organizations, b) seleccionar criterios iniciales, c) obtener documentos formales, d) seleccionar palabras claves, e) formular búsqueda principal.

Preguntas principales: son las preguntas de investigación a continuación

¿Cuáles es la clasificación de los delitos informáticos que afectan a las instituciones?

¿Qué países sufren ataques de delitos informáticos?

¿Qué cantidad de víctimas y valor en dólares se estima en pérdidas por ataques a gobiernos?

¿Cuáles son las medidas preventivas que se recomienda para mitigar los delitos informáticos en Ecuador?

Estrategia de búsqueda: Las librerías digitales para las búsquedas son: ACM Digital Library, IEEE Xplore Digital Library, Springer y Google Scholar

La cadena de búsqueda es: cybercrime OR cybercrime government organizations OR cybercrime Latin America

Tabla 1. Criterios de inclusión y exclusión

Inclusión	**Exclusión**
Artículos de revistas o conferencias	Tesis, monografías, libros
De los últimos 5 años	Artículos duplicados
Solo en idioma inglés o español	Contenido diferente al idioma inglés o español
Informes de organizaciones reconocidas por los gobiernos	

Fuente: Autoría.

4. RESULTADOS

En esta fase se responden las preguntas principales del mapeo sistemático que están planteadas en la metodología.

4.1. Identificación de literatura pertinente en el tema de delincuencia informática

Se aplica el mapeo sistemático y se representa en un PRISMA (Page et al., 2021) para identificar, seleccionar y analizar la literatura pertinente a delincuencia informática, en primera instancia se obtuvo 9264 artículos. Los documentos duplicados están repetidos en las bibliotecas, los documentos no legibles son libros o poster, los documentos removidos por otras razones como vigencia mayor a 5 años, títulos sin relación a delitos informáticos, documentos de pago por ver, documentos de solo resumen.

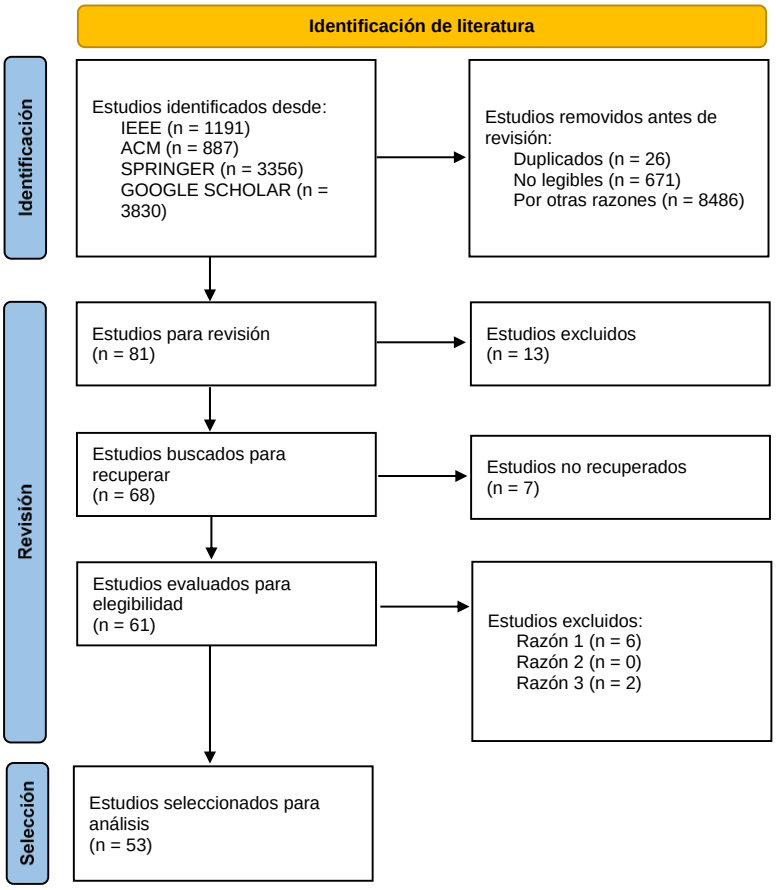


Figura 2. Flujo del diagrama PRISMA

Los estudios para revisión en su resumen son 81, aunque se excluyeron 13 por su literatura gris o documentos con muchas páginas, además no se recuperaron 7 estudios porque piden pago

adicional por bajar el archivo. Entre los estudios a evaluar son 61 aunque en la revisión detalla del documento se descartaron 6 porque son capítulos de libros y otros 2 se descartaron porque su contenido no es ingles ni es español. El resultado son 53 (ver Fig. 2), estos estudios seleccionados se tabulan en una hoja electrónica para responder las preguntas de investigación.

De acuerdo con el mapeo sistemático se obtuvo 53 artículos científicos de las librerías digitales que se presentan en la tabla 2.

Tabla 2. Distribución de estudios científicos

Librería Digital	**Artículos científicos**	**Cantidad**
IEEE	(Batra et al., 2020), (Mallika et al., 2018), (Hamisu et al., 2021), (Toapanta Toapanta et al., 2020), (Amarullah et al., 2021), (Sattar et al., 2019), (Ron et al., 2018), (Yarali & Sahawneh, 2019), (Ahmed et al., 2019), (Kosseff, 2018), (Oni et al., 2019), (Toapanta, Pesantes, et al., 2020), (Toapanta, Ochoa, et al., 2019), (Kapoor et al., 2020), (Tabassum et al., 2018)	15
ACM	(Jirovský et al., 2018), (Onwujekwe et al., 2019), (Mbaziira & Murphy, 2018), (Toapanta, Vaca, et al., 2019), (Toapanta, Jaramillo, et al., 2019), (Toapanta, Peñafiel, et al., 2019)	6
Springer	(Bou Sleiman & Gerdemann, 2021), (Hall et al., 2021), (Yadav et al., 2021), (Oreku & Mtenzi, 2017), (Iqbal et al., 2020), (Velasco, 2022), (Maimon, 2020), (Christopher Westland, 2020), (Dupont, 2017), (Musotto & Wall, 2020), (Hawdon et al., 2020), (Jardine, 2021), (Rehman et al., 2019)	13
Google Scholar	(Maillart, 2019), (Luknar, 2021), (Mariscal et al., 2020), (Izaguirre Olmedo & León Gavilánez, 2018), (Kosevich, 2020), (Kumar & Bhargavi, 2020), (Becerra & Waisbord, 2021), (Izycki, 2019), (Ceron et al., 2021), (Now, 2021), (Hewling, 2018), (Solar, 2020), (Buzzio-Garcia et al., 2021), (Ramírez et al., 2022), (Development, n.d.), (Woodman, 2020), (Hurel, 2022), (Toapanta, Cobeña, et al., 2020), (Bolgov, 2020)	19

Fuente: Autoría.

De acuerdo a literatura de artículos científicos los países que sufren ataques son nombrados por sus afectaciones en delincuencia informática: Brasil es nombrada 11%, México es nombrada 10%, Colombia es nombrada 9%, Chile es nombrada 8%, Argentina y Ecuador en 7% cada uno, Venezuela en 5%, Costa Rica, Paraguay, Perú y Panamá en 4% cada uno, Guatemala y Jamaica en 3% cada uno, Bolivia, Honduras, República Dominicana y Trinidad en 2% cada uno; los demás países son nombrados solo 1% cada uno: Uruguay, Bahamas, Barbados, Barbuda, Belice, Cuba, Granada, Guyana, Haití, Nicaragua, Salvador, San Vicente, Santa Lucía y Surinam (ver Fig. 3).

Este nivel de ataques en Latino América obtenido de los artículos científicos concuerda con las denuncias registradas por el reporte del FBI 2021, aquí Brasil y México son los países de Latinoamérica que están en la lista de los 20 primeros países a nivel mundial con ataques cibernéticos.

Figura 3. Países que sufren ataques en Latino América.

4.2. Clasificación de los delitos informáticos que afectan a las instituciones gubernamentales en Latinoamérica

En el análisis detallado de los 53 artículos científicos se encontró los delitos informáticos que se realizaron en Latinoamérica desde Enero 2017 hasta Marzo 2022; el análisis y clasificación está de acuerdo a (Iqbal et al., 2020) que proporciona información de alto nivel sobre las diversas formas de delitos informáticos, ver Tabla 3.

“El objetivo es el computador”, significa que el delincuente dirige su ataque a los dispositivos de la organización que están en una ubicación segura, puede ser que salga información hacia entornos no confiables o denegación de accesos a la información local o daño al dispositivo.

“Usa el computador como herramienta”, significa que el delincuente utiliza hardware, dispositivos y comunicaciones electrónicas para acoso/seguimiento u obtener información de la organización o apropiación ilegal.

“Crimen como negocio”, significa que el delincuente quiere obtener información para sustraer dinero u otros bienes que puede adquirir con los datos de una persona u organización, engaños para obtener dinero o extorsiones.

“Otros ataques” son los ataques que no entraron en ninguna de tres primeras clasificaciones y que es un delito informático.

Tabla 3. Clasificación de delitos informáticos

Clasificación	Delito informático	Cantidad
El objetivo es el computador	Malware	19
	Virus	10
	Ransonware	8
	Denegación de servicios	20
Usa el computador como herramienta	Acoso	6
	Robo de identidad	5
	Phishing	14
	Información	2
Crimen como Negocio	Suplantación mail	10
	Fraude	13
	Pornografía	8
	Narcotráfico	4
	Difamación	3
	Spoofing	3
	Romance	2
	Hacking	20
	Ingeniería social	6
	Cracking	4
Otros ataques	Otros	16

Fuente: Autoría.

A nivel de detalle el Hacking (20 ocasiones), la Denegación de Servicios (20 ocasiones) y el Malware (19 ocasiones) son los delitos informáticos con mayor incidencia obtenidos en esta investigación, estos pertenecen a la clasificación de “el objetivo es el computador”, al “uso del computador como herramienta” y al “crimen como negocio” respectivamente; esto quiere decir que las tres clasificaciones tienen un factor importante cada uno (ver Fig. 4).

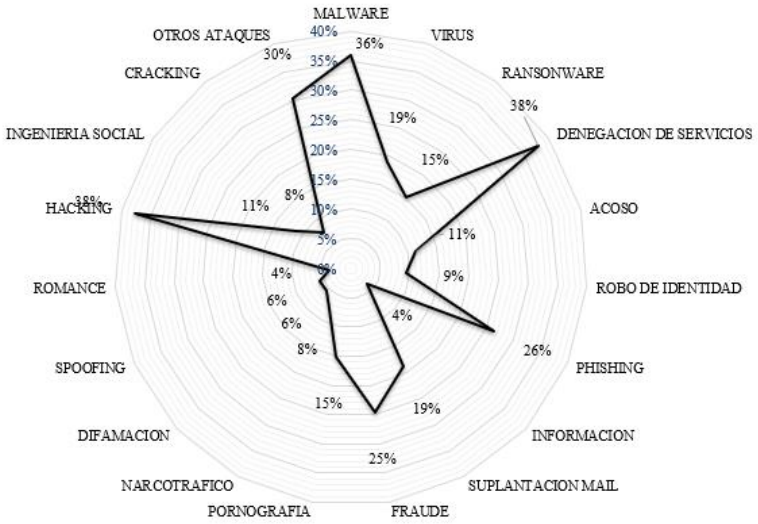


Figura 4. Clasificación de los ataques en Latino América.

En los 53 artículos, el tipo "Crimen como negocio" es el primer ataque que se realiza en organizaciones de América Latina con 42%, el tipo "Objetivo es el computador" es el segundo tipo de ataque con 33%, el tipo "Usa el computador como herramienta" ocurre en 16%, y los demás ataques ocurren en 9%. Esto quiere decir que la extracción de dinero es la prioridad para los delincuentes informáticos (ver Fig. 5).

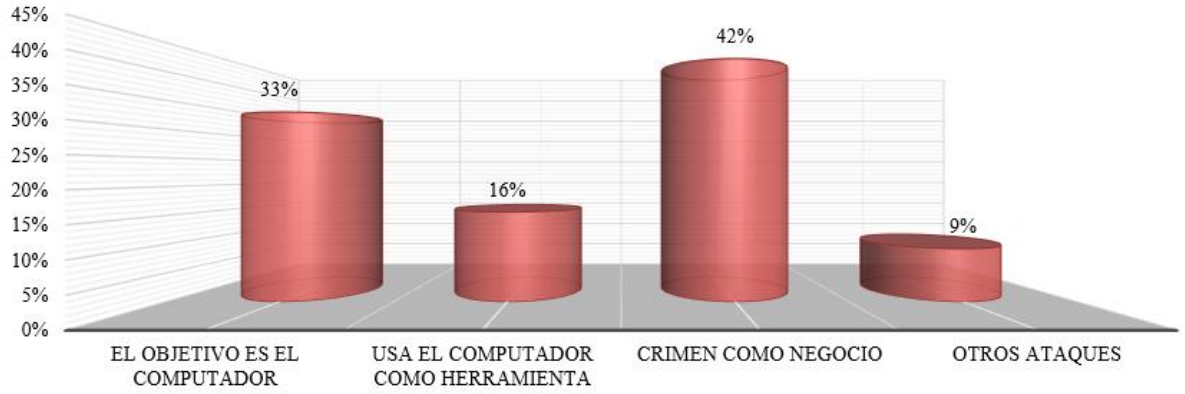


Figura 5. Clasificación de los ataques en Latino América.

De acuerdo con las denuncias realizadas en el FBI desde el año 2017 al 2021 existen 58162 víctimas y 452 millones de dólares en un delito informático específico llamado Suplantación de Gobierno (FBI, 2021) que una afectación directa a un gobierno por una persona para obtener dinero de los contribuyentes u obtener dinero de una organización pública. En los últimos cinco años la cantidad de dinero aumentó, en 2021 la cantidad de delitos disminuyó a 11335 delitos informáticos pero la cantidad de dinero se incrementó a 142 millones de dólares en esta clase de delito (ver Fig. 6).

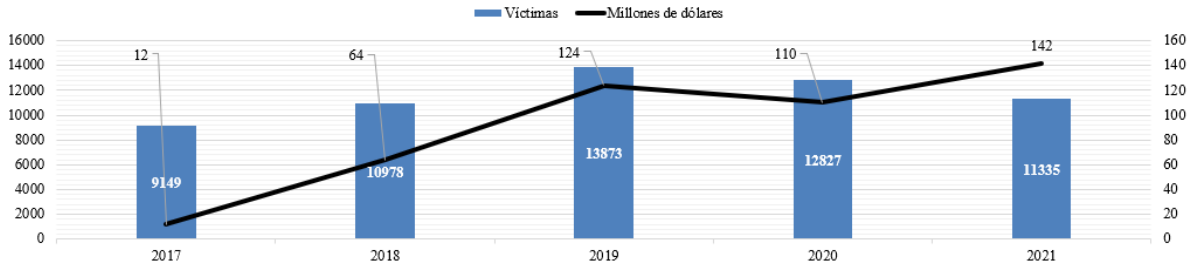


Figura 6. Ataques a gobiernos o ataques a nombre de gobiernos.

4.3. Contraste de los resultados obtenidos para proteger la información en las instituciones gubernamentales en Ecuador

De acuerdo con los datos tabulados de los artículos en la hoja electrónica se hallaron medidas que las organizaciones toman para prevenir los ataques, la Tabla 4 en las columnas están las medidas preventivas con las referencias que nombran la prevención, se las ordena de menor a mayor: la prevención más utilizada es la legislación en 25 artículos, los sistemas de terceros en 19 artículos, crear Framework propio en 11 artículos, crear departamentos especializados en 7 artículos, aplicar Inteligencia Artificial en 5 artículos, aplicar Encriptación a la información en 4 artículos, aplicar Big Data en 3 artículos, tener sistemas de Autenticación en 2 artículos, y aplicar Hacking ético en 1 artículo.

Tabla 4. Medidas preventivas contra delitos informáticos

Hacking ético	Concientización	Autenticación	Data mining o big data	Encriptación a información	Inteligencia artificial	Departamentos	Framework propio	Sistema de terceros	Legislación
(Toapanta Toapanta et al., 2020)	(Ahmed et al., 2019)	(Toapanta Toapanta et al., 2020)	(Batra et al., 2020)	(Ron et al., 2018)	(Batra et al., 2020)	(Ron et al., 2018)	(Mallika et al., 2018)	(Mallika et al., 2018)	(Ron et al., 2018)
	(Luknar, 2021)	(Kosseff, 2018)	(Jirovský et al., 2018)	(Christopher Westland, 2020)	(Mbaziira & Murphy, 2018)	(Yarali & Sahawneh, 2019)	(Toapanta, Vaca, et al., 2019)	(Toapanta Toapanta et al., 2020)	(Oni et al., 2019)
		(Buzzio-Garcia et al., 2021)	(Onwujekwe et al., 2019)	(Mariscal et al., 2020)	(Iqbal et al., 2020)	(Iqbal et al., 2020)	(Toapanta, Jaramillo, et al., 2019)	(Ron et al., 2018)	(Yarali & Sahawneh, 2019)
				(Buzzio-Garcia et al., 2021)	(Velasco, 2022)	(Christopher Westland, 2020)	(Toapanta, Peñafiel, et al., 2019)	(Oni et al., 2019)	(Sattar et al., 2019)
					(Mariscal et al., 2020)	(Kosevich, 2020)	(Oreku & Mtenzi, 2017)	(Ahmed et al., 2019)	(Kosseff, 2018)
						(Buzzio-Garcia et al., 2021)	(Iqbal et al., 2020)	(Toapanta, Pesantes, et al., 2020)	(Tabassum et al., 2018)
						(Hurel, 2022)	(Jardine, 2021)	(Toapanta, Ochoa, et al., 2019)	(Bou Sleiman & Gerdemann, 2021)

(Bolgov, 2020)	(Kumar & Bhargavi, 2020)	(Kosseff, 2018)	(Hall et al., 2021)
	(Ceron et al., 2021)	(Tabassum et al., 2018)	(Yadav et al., 2021)
	(Hewling, 2018)	(Maimon, 2020)	(Oreku & Mtenzi, 2017)
	(Toapanta Toapanta et al., 2020)	(Dupont, 2017)	(Iqbal et al., 2020)
		(Musotto & Wall, 2020)	(Jardine, 2021)
		(Rehman et al., 2019)	(Maillart, 2019)
		(Mariscal et al., 2020)	(Izaguirre Olmedo & León Gavilánez, 2018)
		(Izaguirre Olmedo & León Gavilánez, 2018)	(Kosevich, 2020)
		(Buzzio-Garcia et al., 2021)	(Becerra & Waisbord, 2021)
		(Development, n.d.)	(Izycki, 2019)
		(Woodman, 2020)	(Now, 2021)
		(Hurel, 2022)	(Solar, 2020)
			(Ramírez et al., 2022)
			(Development, n.d.)
			(Woodman, 2020)
			(Hurel, 2022)
			(Toapanta Toapanta et al., 2020)
			(Bolgov, 2020)

Fuente: Autoría.

La representación porcentual de las unidades literarias que nombran las medidas preventivas contra los ataques y que se recomienda para Ecuador es: la Legislación o acciones legales es la prevención más utilizada con 31%, segundo lugar es la utilización de sistemas que pertenecen a terceros que son soluciones comerciales con 23%, tercer lugar es el desarrollo de framework propio con 14%, cuarto lugar está la creación de secciones departamentales con personal especializado en protección de información en 10%, luego está el uso de inteligencia artificial, encriptación, Big data, autenticación, concientización y hacking ético con 6%, 5%, 4%, 4%, 2% y 1% respectivamente cada uno (ver Fig. 7).

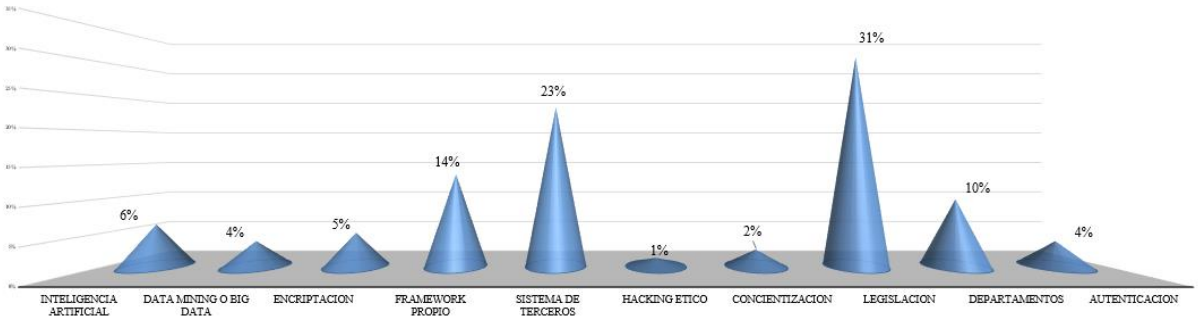


Figura 7. Ataques a nombre de gobiernos

5. DISCUSIÓN

El desarrollo de la informática, redes e internet tiene alto impacto en las personas y empresas privadas o públicas, uso TIC tiene un impacto potencial en la seguridad de la información, porque la distribución de la información es más sencilla y económica; en la misma magnitud los delincuentes informáticos están al acecho de las personas e instituciones para dañar la información o infraestructura.

Existe una la necesidad del mejorar la seguridad de información, seguridad de conexiones y seguridad de computadores, no solo tener protección defensiva además es necesario que los gobiernos tengan prevención proactiva para encontrar los orígenes y objetivos de los delincuentes informáticos.

Se destaca que las condiciones de los delitos informáticos son diferentes a las condiciones de los delitos comunes, y el nivel socioeconómico está relacionado con el conocimiento para realizar un delito. Es necesario educar a las personas en las organizaciones gubernamentales para mitigar o minimizar los ataques informáticos, aunque no todos acatan las disposiciones.

Si un ataque informático tiene éxito en una organización gubernamental el impacto es económico por pérdida de tiempo, es social por la desatención a los ciudadanos, es político por la imagen del gobierno de turno.

En esta investigación se clasificaron los delitos informáticos y las medidas de prevención para mitigar el impacto, no se presentan precios de herramientas informáticas, ni costos de los delitos informáticos en las organizaciones de un solo gobierno, sino a nivel global. Las preguntas principales del mapeo sistemático son respondidas en los resultados

En Latinoamérica, Brasil está en primer lugar de hechos por delitos informáticos y Ecuador está sexto lugar, se obtuvo 18 delitos informáticos más comunes, los delitos no nombrados están en otros ataques.

6. CONCLUSIÓN

Mediante el mapeo sistemático se identificaron variedad de documentos y se obtuvo 53 artículos científicos de cuatro bibliotecas digitales, cabe recalcar que 70% de los documentos realizan estudios sobre el mundo y Latinoamérica, el 30% de los documentos son de países de Latinoamérica. El 68% de todos los documentos realizan análisis sobre los delitos informáticos.

Se obtuvo cuatro clasificaciones de los delitos informáticos que afectan a todo tipo de empresas e instituciones gubernamentales, el Crimen como Negocio es la clasificación más nombrada.

Se obtuvo las medidas preventivas que las empresas e instituciones gubernamentales utilizan para proteger la información es la “Legislación” para ejecutar acciones legales sobre los infractores es la más utilizada, y es la recomendada para Ecuador seguido de las otras medidas.

REFERENCIAS

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20566

Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019). Demographic factors of cybersecurity awareness in Bangladesh. *2019 5th International Conference on Advances in Electrical Engineering, ICAEE 2019, June 2018*, 685–690. https://doi.org/10.1109/ICAEE48663.2019.8975603

Alvarado Ronquillo, M. L. (2021). *Analysis for the adoption of security standards to improve the management of securities in public organizations*. https://dspace.ups.edu.ec/handle/123456789/19760

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analyzing Cyber Crimes during COVID-19 Time in Indonesia. *2021 3rd International Conference on Computer Communication and the Internet, ICCCI 2021*, 78–83. https://doi.org/10.1109/ICCCI51764.2021.9486775

Ayala Carabajo, R., & Llerena Izquierdo, J. (2017). *Tercer Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad*. https://dspace.ups.edu.ec/handle/123456789/14450

Ayala Carabajo, R., Llerena Izquierdo, J., Parra, P., Vega Ureta, N., Hernández, A., Romero, I., Silva, J., Rojas, T., Pérez Gosende, P., Yaguana, T., Cueva, J., Sumba, N., Gonzaga Acuña, A., López Chila, R., Caballero, E., Portugal, D., Medina, F., Mendieta, N., Caamaño, L., … Parra, P. (2016). *Segundo Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad Memoria académica*. http://dspace.ups.edu.ec/handle/123456789/12776

Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020). An empirical study of cybercrime and its preventions. *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, 42–46. https://doi.org/10.1109/PDGC50313.2020.9315785

Becerra, M., & Waisbord, S. R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public*, *6*(1–4), 67–79. https://doi.org/10.1177/20570473211046730

Bolgov, R. (2020). The UN and Cybersecurity Policy of Latin American Countries. *2020 7th International Conference on EDemocracy and EGovernment, ICEDEG 2020*, 259–263. https://doi.org/10.1109/ICEDEG48599.2020.9096798

Bou Sleiman, M., & Gerdemann, S. (2021). Covid-19: a catalyst for cybercrime? *International Cybersecurity Law Review*, *2*(1), 37–45. https://doi.org/10.1365/s43439-021-00024-9

Buzzio-Garcia, J., Salazar-Vilchez, V., Moreno-Torres, J., & Leon-Estofanero, O. (2021). Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview. *ETCM 2021 - 5th Ecuador Technical Chapters Meeting*. https://doi.org/10.1109/ETCM53643.2021.9590693

Ceron, W., Gruszynski Sanseverino, G., de-Lima-Santos, M. F., & Quiles, M. G. (2021). COVID-19 fake news diffusion across Latin America. *Social Network Analysis and Mining*, *11*(1), 1–20. https://doi.org/10.1007/s13278-021-00753-z

Chévez Morán, M. J. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*. http://dspace.ups.edu.ec/handle/123456789/20568

Christopher Westland, J. (2020). *Blockchains, Cybercrime, and Forensics*. *2008*, 279–290. https://doi.org/10.1007/978-3-030-49091-1_11

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

de la Nube Toral Sarmiento, A., Loaiza Martínez, M. de L., Llerena Izquierdo, J., Ayala Carabajo, R., Torres Toukoumidis, A., Romero-Rodríguez, L. M., Aguaded, I., Vega Ureta, N. T., Fuentes Espinoza, P. G., Peñafiel Caicedo, J. A., & others. (2018). *4to. Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad. Memoria académica*. http://dspace.ups.edu.ec/handle/123456789/16318

De Oliveira, T. R., Da Silva, M. M., Spinasse, R. A. N., Ludke, G. G., Gaudio, M. R. S., Gomes, G. I. R., Cotini, L. G., Vargens, D., Schimidt, M. Q., Andreao, R. V., & Mestria, M. (2021). Systematic Review of Virtual Reality Solutions Employing Artificial Intelligence Methods. *ACM International Conference Proceeding Series*, 42–55. https://doi.org/10.1145/3488162.3488209

Development, P. (n.d.). *Cybersecurity and the role of the Board of Directors in Latin America*.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116. https://doi.org/10.1007/s10611-016-9649-z

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

FBI. (2021). 2021-Internet Crime Report. In *Federal Bureau of Investigation - Internet Crime Complaint Center* (Issue I).

Guaigua Bucheli, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20319

Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: the multiscalar production of cybercrime. *Trends in Organized Crime*, *24*(2), 282–307. https://doi.org/10.1007/s12117-020-09392-w

Hamisu, M., Idris, A. M., Mansour, A., & Olalere, M. (2021). Analysis of cybercrime in Nigeria. *Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace, CYBER NIGERIA 2020*, 73–79. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428848

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*, *45*(4), 546–562. https://doi.org/10.1007/s12103-020-09534-4

Hewling, M. (2018). Cyber intelligence: A framework for the sharing of data. *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, *2018-March*, 637–644.

Holguín Mendoza, J. D. (2021). *Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20915

Hurel, L. M. (2022). Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America. *Global Security Review*, *2*(1). https://doi.org/10.25148/gsr.2.009786

Iqbal, F., Debbabi, M., & Fung, B. C. M. (2020). *Cybersecurity And Cybercrime Investigation*. 1–21. https://doi.org/10.1007/978-3-030-61675-5_1

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Analysis of cyber-attacks carried out in Latin America. *INNOVA Research Journal*, *3*(9), 180–189. https://doi.org/10.33890/innova.v3.n9.2018.837

Izycki, E. (2019). *National Cyber Security Strategies in Latin America*. *April 2018*.

Jardine, E. (2021). Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice*, *46*(6), 980–1005. https://doi.org/10.1007/s12103-021-09656-3

Jirovský, V., Mühlhäuser, M., Pastorek, A., & Tundis, A. (2018). Cybercrime and organized crime. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3233288

Kapoor, P., Singh, P. K., & Cherukuri, A. K. (2020). IT Act Crime Pattern Analysis using Regression and Correlation Matrix. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 1102–1106. https://doi.org/10.1109/ICRITO48877.2020.9197835

Kosevich, E. (2020). Cyber Security Strategies of Latin America Countries. *IBEROAMERICA*, *1*, 137–159. https://doi.org/10.37656/s20768400-2020-1-07

Kosseff, J. (2018). Developing collaborative and cohesive cybersecurity legal principles. *2018 10th International Conference on Cyber Conflict (CyCon)*, *2018-May*, 283–298. https://doi.org/10.23919/CYCON.2018.8405022

Kumar, M. K., & Bhargavi, D. K. (2020). An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. *Journal of Engineering, Computing and …*, *July*.

Luknar, I. (2021). *Cyberterrorism threat and the pandemic*. *November*. https://doi.org/10.20544/ICP.11.01.20.p29

Maillart, J. B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, *19*(3), 375–390. https://doi.org/10.1007/s12027-018-0527-2

Maimon, D. (2020). Relevance of Evidence-Based Cybersecurity in Guiding the Financial Sector's and Efforts in Fighting Cybercrime. In *Countering Cyber Threats to Financial Institutions* (Issue 1984, pp. 9–28). Springer International Publishing. https://doi.org/10.1007/978-3-030-54054-8_2

Mallika, Deep, V., & Sharma, P. (2018). Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study. *Proceedings of the International Conference on Computational Techniques, Electronics and Mechanical Systems, CTEMS 2018*, 499–503. https://doi.org/10.1109/CTEMS.2018.8769140

Mariscal, J., Davó, G. M., & Rio, A. R. del. (2020). *Strengthening cyber policy research centers in the global south (Latin America and the Caribbean)*.

Mbaziira, A. V., & Murphy, D. R. (2018). An empirical study on detecting deception and cybercrime using artificial neural networks. *ACM International Conference Proceeding Series*, 42–46. https://doi.org/10.1145/3193077.3193080

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20243

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS 1. Hawdon, J., Parti, K., Dearden, T.E.: Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. Am. J. Crim. Justice. 45, 546–562 (2020). https://doi.org/10.1007/s12103-020-09534-4stres. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-020-09397-5

Now, A. (2021). *The persecution of the information security community in LATAM*.

Oni, S., Araife Berepubo, K., Atinuke Oni, A., & Joshua, S. (2019). E-government and the challenge of cybercrime in Nigeria. *2019 6th International Conference on EDemocracy and EGovernment, ICEDEG 2019*, 137–142. https://doi.org/10.1109/ICEDEG.2019.8734329

Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019). Using robust data governance to mitigate the impact of cybercrime. *ACM International Conference Proceeding Series*, 70–79. https://doi.org/10.1145/3325917.3325923

Oreku, G. S., & Mtenzi, F. J. (2017). *Cybercrime : Concerns , Challenges and Opportunities*. 129–153. https://doi.org/10.1007/978-3-319-44257-0

Orozco Bonilla, C. A. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/20933

Page, M. J., McKenzie, J. E., & Bossuyt, P. M. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery*, *88*, 1–11. https://doi.org/10.1016/j.ijsu.2021.105906

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*. http://dspace.ups.edu.ec/handle/123456789/20937

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability*, *14*(3), 1390. https://doi.org/10.3390/su14031390

Rehman, H. ur, Yafi, E., Nazir, M., & Mustafa, K. (2019). Security Assurance Against Cybercrime Ransomware. *Advances in Intelligent Systems and Computing*, *866*, 21–34. https://doi.org/10.1007/978-3-030-00979-3_3

Ron, M., Fuertes, W., Bonilla, M., Toulkeridis, T., & Diaz, J. (2018). Cybercrime in Ecuador, an exploration, which allows to define national cybersecurity policies. *Iberian Conference on Information Systems and Technologies, CISTI*, *2018-June*, 1–7. https://doi.org/10.23919/CISTI.2018.8399357

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21699

Sandjojo, N., Zuhriyanto, M., & Pradnyana, I. W. W. (2020). The Effects of Fear of Cybercrime and Information Systems Security Policy on National Vigilance. *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, 195–200. https://doi.org/10.1109/ICIMCIS51567.2020.9354283

Sattar, Z., Riaz, S., Shafia, & Mian, A. U. (2019). Challenges of cybercrimes to implementation of legal framework. *2018 14th International Conference on Emerging Technologies, ICET 2018*. https://doi.org/10.1109/ICET.2018.8603645

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392–412. https://doi.org/10.1080/23738871.2020.1820546

Tabassum, A., Mustafa, M. S., & Maadeed, S. A. Al. (2018). The need for a global response against cybercrime: Qatar as a case study. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, *2018-Janua*, 1–6. https://doi.org/10.1109/ISDFS.2018.8355331

Tacuri López, I. L. (2021). *Acoso por medio de las tecnologías en las redes sociales durante*

tiempos de pandemia en Ecuador, una revisión sistemática. http://dspace.ups.edu.ec/handle/123456789/20242

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático*. https://dspace.ups.edu.ec/handle/123456789/20333

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*. http://dspace.ups.edu.ec/handle/123456789/20942

Toapanta, S. M. T., Cobeña, J. D. L., & Gallegos, L. E. M. (2020). Analysis of cyberattacks in public organizations in Latin America. *Advances in Science, Technology and Engineering Systems*, *5*(2), 116–125. https://doi.org/10.25046/aj050215

Toapanta, S. M. T., Jaramillo, J. M. E., & Gallegos, L. E. M. (2019). Cybersecurity analysis to determine the impact on the social area in Latin America and the caribbean. *ACM International Conference Proceeding Series*, 73–78. https://doi.org/10.1145/3375900.3375911

Toapanta, S. M. T., Ochoa, I. N. C., Sanchez, R. A. N., & Mafla, L. E. G. (2019). Impact on administrative processes by cyberattacks in a public organization of Ecuador. *Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019*, 270–274. https://doi.org/10.1109/WorldS4.2019.8903967

Toapanta, S. M. T., Peñafiel, L. B., & Gallegos, L. E. M. (2019). Prototype to mitigate the risks of the integrity of cyberattack information in electoral processes in Latin America. *ACM International Conference Proceeding Series*, 111–118. https://doi.org/10.1145/3375900.3375915

Toapanta, S. M. T., Pesantes, R. P. R., & Gallegos, L. E. M. (2020). Impact of Cybersecurity Applied to IoT in Public Organizations in Latin America. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 154–161. https://doi.org/10.1109/WorldS450073.2020.9210416

Toapanta, S. M. T., Vaca, A. J., & Gallegos, L. E. M. (2019). Design of a prototype for IT security architectures in a public organization for Latin America. *ACM International Conference Proceeding Series*, 119–124. https://doi.org/10.1145/3375900.3375916

Toapanta Toapanta, S. M., Mera Caicedo, H. A., Naranjo Sanchez, B. A., & Mafla Gallegos, L. E. (2020). Analysis of security mechanisms to mitigate hacker attacks to improve e-commerce management in Ecuador. *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, 242–250. https://doi.org/10.1109/ICICT50521.2020.00044

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, *Dc*. https://doi.org/10.1007/s12027-022-00702-z

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. http://dspace.ups.edu.ec/handle/123456789/20949

Woodman, S. (2020). Hackers paradise. *Index on Censorship*, *49*(2), 40–42. https://doi.org/10.1177/0306422020935798

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). Various Types of Cybercrime and Its Affected Area. In *Lecture Notes in Networks and Systems* (Vol. 164). Springer Singapore. https://doi.org/10.1007/978-981-15-9774-9_30

Yarali, A., & Sahawneh, F. G. (2019). Deception: Technologies and Strategy for Cybersecurity. *Proceedings - 4th IEEE International Conference on Smart Cloud, SmartCloud 2019 and 3rd International Symposium on Reinforcement Learning, ISRL 2019*, 110–120.

https://doi.org/10.1109/SmartCloud.2019.00029