Revista científica Portal de la Ciencia

ISSN: 2953-6502

Fecha de presentación: 17/06/2024
Fecha de aceptación: 18/08/2024
Fecha de publicación: 01/09/2024

Fabian Andrés Castañeda-Ortega
E-mail: fabian.castaneda@fuac.edu.co
Orcid: https://orcid.org/0009-0000-6728-1570

Fiscalía General de la Nación, Colombia

Cita sugerida (APA, séptima edición)

Castañeda-Ortega, F. A. (2024). Ciberdelincuencia: análisis de tendencias y estrategias de mitigación, caso Colombia. *Revista Portal de la Ciencia*, 5(3), 298-308, DOI: https://doi.org/10.51247/pdlc.v5i3.474.

==== o ====

Ciberdelincuencia: análisis de tendencias y estrategias de mitigación, caso Colombia.

RESUMEN.

El ciberdelito, una realidad global de gran envergadura, comprende actividades delictivas perpetradas mediante medios electrónicos y redes informáticas. En Colombia, esta modalidad se emplea para vulnerar las bases de datos de la fiscalía general de la nación, entidad encargada de investigar y presentar cargos ante los tribunales competentes contra aquellos sospechosos de haber cometido conductas criminales que amenacen la vida, seguridad o propiedades de las personas. Es de anotar que esta actividad criminal tiene como finalidad obtener ganancias financieras, esto debido a la utilización de programas maliciosos para acceder a la información sensible de las personas vinculadas en procesos judiciales y cuya información está asentada en las bases de datos Fiscalía General de la Nación de Colombia los ciberdelincuentes utilizan diversas técnicas, como el malware o ataques de denegación de servicios para comprometer los sistemas informáticos de la Fiscalía General de la Nación.

Palabras clave: ciberdelito, ciberseguridad, ingeniería social, jurisprudencia

==== o ====

Cybercrime: analysis of trends and mitigation strategies, case of Colombia.

ABSTRACT

Cybercrime, a global reality of significant magnitude, encompasses criminal activities perpetrated through electronic means and computer networks. In Colombia, this modality is used to breach the databases of the Office of the Attorney General, an entity responsible for investigating and presenting charges before competent courts against those suspected of committing criminal conduct that threatens the life, security, or property of individuals. It is noteworthy that this criminal activity aims to obtain financial gains, achieved through the use

of malicious programs to access the sensitive information of individuals involved in legal processes and whose information is stored in the databases of the Office of the Attorney General of Colombia. Cybercriminals use various techniques, such as malware or denial-of-service attacks, to compromise the computer systems of the Office of the Attorney General.

Keywords: cybercrime, cybersecurity, social engineering, jurisprudence.

==== o ====

Crime cibernético: análise de tendências e estratégias de mitigação, caso Colômbia.

RESUMO

O cibercrime, uma realidade global em grande escala, inclui atividades criminosas perpetradas através de meios eletrónicos e redes informáticas. Na Colômbia, esta modalidade é utilizada para violar as bases de dados da Procuradoria-Geral do país, entidade encarregada de investigar e apresentar acusações perante os tribunais competentes contra os suspeitos de terem cometido condutas criminosas que ameaçam a vida, a segurança ou a propriedade das pessoas. Refira-se que o objectivo desta actividade criminosa é a obtenção de ganhos financeiros, devido à utilização de programas maliciosos para aceder a informação sensível de pessoas envolvidas em processos judiciais e cujas informações estão armazenadas nas bases de dados da Procuradoria-Geral da República. Na Colômbia, os cibercriminosos utilizam diversas técnicas, como malware ou ataques de negação de serviço, para comprometer os sistemas informáticos da Procuradoria-Geral da República.

Palavras-chave: crime cibernético, segurança Cibernética, engenharia social, jurisprudência

==== o ====

INTRODUCCIÓN.

En la era digital actual, el ciberdelito es una preocupación creciente a nivel mundial. La complejidad y diversidad de las amenazas cibernéticas requieren que las personas, las empresas y los gobiernos comprendan y respondan de manera efectiva. El propósito de este artículo es abordar el fenómeno del ciberdelito de manera sistemática, comenzando por su definición y alcance, y luego examinando sus diversas manifestaciones, motivaciones y consecuencias. Esto con el fin de proporcionar una visión comprensiva y estructurada de esta compleja problemática, se procederá a clasificar las distintas categorías de ciberdelitos, jerarquizar las amenazas según su impacto y frecuencia, seleccionar casos representativos para el análisis detallado y, finalmente, ordenar el contenido de manera lógica. Este método secuencial permitirá un análisis y comprensión más profundos del ciberdelito y su impacto en la sociedad moderna.

En este artículo, se examinan los aspectos claves del ciberdelito, sus implicaciones y las estrategias para mitigar sus efectos todo esto siguiendo las experiencias vividas por muchas personas a quienes el ciberdelito les genero alguna afectación. La investigación se centra en la comprensión de los tipos específicos de ciberdelitos y sus motivaciones subyacentes. Se ha recurrido a una amplia gama de fuentes bibliográficas, incluidos libros, artículos académicos y estudios de casos recientes, para contextualizar y respaldar esta investigación. La elección de literatura actualizada y novedosa se basa en la necesidad de comprender los desafíos y las tendencias emergentes en el campo del ciberdelito.

Esto incluye el análisis de nuevas tecnologías, tácticas de ataque innovadoras y cambios en el panorama de las amenazas cibernéticas. Al recurrir a un apoyo bibliográfico actualizado y novedoso, se busca proporcionar una base sólida para la investigación y garantizar que los hallazgos y conclusiones sean relevantes y aplicables en el contexto actual del ciberespacio.

Actualmente las tendencias en las distintas organizaciones criminales utilizan las nuevas tecnologías para poner en común sus recursos y su experiencia. Así, el Delito Informático o bien el Cibercrimen, hace referencia a todo ataque usando como medio un ordenador y/o internet. En Colombia, en el primer año de pandemia, aumentaron los ciberdelitos de manera exponencial y en 2021 se multiplicaron por diez. Se monitorearon más de 3.700 millones de intentos de ciberataque en la primera mitad del año 2021; solo a finales del año 2020, se presentó un incremento del 440% en uso de campañas de phishing a nivel mundial.

La relevancia de este flagelo es que ha venido afectando a la población mundial donde ha generado consecuencias graves a las víctimas de los ciberataques, con el pasar del tiempo se están capacitando al personal de los diferentes organismos de seguridad con el fin de neutralizar a estos facinerosos y desmantelar estas organizaciones delincuenciales, pare ello recolectan Elementos Materiales Probatorios y/o Evidencia Física que permita determinar la posible participación de estas personas en la comisión de actividades delictivas, relacionadas con el cibercrimen o ciberdelito.

Es importante concientizar y capacitar a la sociedad en el manejo de las tecnologías para que estos desarrollen habilidades con el objetivo de aprender a extremar las medidas de seguridad en su información personal para que estos no caigan incautos a los engaños de la persona que se encentra detrás de otro ordenador.

Marco legal o normativo – legislación colombiana

- Constitución Política de Colombia Artículo No. 15
- Ley 599 de 2000 – Código Penal Colombiano
- Ley 906 de 2005 – Código de Procedimiento Penal.
- Ley 1273 de 2009 – Ley de Delitos Informáticos.
- Convenio de Budapest de 2001 – Convenio Contra la Cibercriminalidad.
- Ley 1928 de 2018 – Aprobación del Convenio de Budapest en Colombia.

MARCO TEÓRICO Y CONCEPTUAL

¿Qué es la Seguridad Informática?

Numerosas compañías, tanto privadas como de orden público, están sometidas cada vez más a la tecnología informática al avanzar de manera acelerada, con el fin de llevar a cabo sus actividades esenciales, no solo en la administración del capital económico y humano, sino también para la adecuada prestación de sus servicios.

En contexto, Maya (2017) afirma que, *Los cibercrímenes son delitos con características particulares por lo que corresponde a la acción, el sujeto, el resultado y su imputación.* Por otra parte, Agustina, J. R. (2021) afirma que:

> *"La tecnología y el Derecho penal parecen, pues, estar llamados a entablar un diálogo fluido y entenderse a fondo si se pretende hacer frente al efecto desplazamiento de una buena parte de las infracciones penales a ese nuevo lugar o espacio sui generis, donde el principio de territorialidad de la ley penal cada vez plantea más inconvenientes." (Agustina, J. R. (2021)*

A su vez Palacios (2021) menciona que:

> *"Los delitos que atentan contra los datos e informaciones en el plano informático representan una flagrante vulneración de uno de los derechos más fundamentales de la persona: su intimidad. Por ello, indica que resulta muy importante realizar estudios más profundos y con mayor LIBRO DE ESTUDIOS DE CASOS 104 alcance que permitan abordar jurídica y legalmente la naturaleza intangible e imputabilidad de los ciberdelitos, así como sus implicancias en los derechos fundamentales, si se tiene en cuenta que el referido ilícito dispone de autonomía frente al Código Penal vigente." (Palacios, 2021)*

Dentro del estudio del estudio del ciberdelito se puede determinar que el ciberdelito es un fenómeno mundial de alto nivel que implica actividades delictivas realizadas por medios electrónicos y redes informáticas. Hay que mencionar, además que Antonio Rodríguez, J., Oduber, J., & Mora, E. (2017) El ciberdelito ha aumentado significativamente a nivel mundial en estas últimas décadas. En tal sentido, la investigación sobre este fenómeno en Venezuela ha sido escasa, específicamente en lo que respecta a los factores asociados con la victimización en línea. Considerando las palabras de A. Rodríguez, J., Oduber, J., y Mora, E. (2017)

"Cibervictimización y actividades rutinarias: desarrollos teóricos y empíricos La victimización en línea se ha estudiado fundamentalmente en los países desarrollados en las dos últimas décadas. Con el propósito de recopilar información, evaluarla y, luego, tratar de predecir y explicar los delitos relaciona-dos con las TIC, algunos trabajos se han dedicado a analizar el significado y la naturaleza de múltiples formas de ciberdelitos. Al punto que, en un marco de visibles desacuerdos, los expertos en el tema han propuesto diferentes definiciones de lo que puede entenderse por delito informático y creado a partir de ellas algunas tipologías."

En Un estudio realizado por Feld, (2017), donde examina detalladamente cómo los avances tecnológicos y la evolución de los delitos cibernéticos han desafiado las tradicionales teorías del delito y la justicia penal. Feld sostiene que el concepto de ciberdelito, definido como la participación indirecta o complicidad en un delito a través de medios digitales, plantea nuevas preguntas sobre la responsabilidad y la imputación en un mundo cada vez más interconectado y tecnológicamente avanzado. Este autor argumenta que la comprensión y regulación efectiva de los ciberdelitos requiere una revisión exhaustiva de los marcos legales y las políticas de justicia penal.

Así mismo para Gamón, V. P. (2017). En donde establece consideraciones metodológicas:

"La investigación consiste en evaluar la seguridad ciudadana de la República de Panamá en los periodos de gobierno 2004-2009 y 2009- 2019 a través de un Modelo que adopta un enfoque institucional cualitativo acotado de la seguridad ciudadana que se circunscribe al análisis y evaluación de tres dimensiones específicas de la seguridad y de la política general gubernamental en esta materia, y en la que se consideran entidades, aspectos e instrumentos de control, administración, sanción y prevención de la violencia y la criminalidad."

Las dimensiones consideradas para este estudio son las siguientes: dimensión de las Instituciones del Sistema de Justicia Penal, dimensión Regulativa de la Seguridad Pública, y la dimensión de las Estrategias de Política Gubernamental y de Programas Preventivos. En este artículo, describiremos y presentaremos los resultados de la evaluación de la primera dimensión del modelo de análisis planteado (. . .) (Gamón, 2017)

Es importante señalar a Cedeño Villacís R. P. (2022). Ciberseguridad y Ciberdefensa:

> *"En Abril del 2019, el gobierno del Ecuador tomó la decisión de dar por terminado el asilo el a Julián Assange en la embajada ubicada en Londres; esto provocó que el país sufriera atentados cibernéticos, los cuales llegaron a 40 millones de ataques causados por delincuentes informáticos; el objetivo fue saturar los sitios web con el*

> *propósito de impedir que los usuarios puedan acceder a estos, este tipo de ataque es llamado denegación de servicio –DoS (El Comercio, 2019).”*
>
> *“Decenas de hackers participaron de este ciberataque, con la intención de provocar afectación a la infraestructura tecnológica de las entidades del estado; de acuerdo con los datos estadísiticos de Kapersky de las ciber amenazas en tiempo real, el Ecuador, que ocupaba el puesto 56 subió hasta el 25 en el ranking de los países más vulnerables en el mundo, en apenas pocas horas (Expreso, 2019). (…) (Cedeño Villacís R. P, 2022).”*

Por consiguiente, para Mayer Lux, Laura. (2018). Es importante relacionar que el

> *“Pese a que las estadísticas sobre denuncias y condenas pueden ser útiles para comprender y explicar algunos aspectos criminológicos involucrados en la delincuencia informática, su valor no debe sobreestimarse. Los delitos informáticos que son conocidos en el sistema procesal penal representan sólo una parte de la criminalidad informática, cuyas efectivas dimensiones son muy difíciles de precisar, entre otras razones, por los problemas que enfrentan su denuncia, investigación y juzgamiento32".*
>
> *“En la misma línea, las sentencias chilenas sobre conductas subsumibles en la Ley Nº 19.223 son escasas y no siempre aportan luces sobre los medios y contextos de ejecución, los autores y víctimas, o las consecuencias de dichos ilícitos. De ahí que su referencia se circunscriba a aquellos aspectos de los casos fallados que, más allá de su calificación jurídica, puedan resultar de interés para el análisis criminológico de tales delitos.”*

Ahora bien, de acuerdo con Vinelli Vereau, R. (2021).

> *“Es pertinente mencionar que los delitos informáticos o cibercrímenes también fueron parte de la agenda del Décimo Segundo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, llevado a cabo del 12 al 19 de abril del 2010 en la ciudad de Salvador en Brasil. En este congreso internacional se debatió la problemática de los delitos informáticos. Al respecto, se recalcó que el delito cibernético era uno de los mayores problemas que afrontaban los órganos de aplicación de la ley y se señaló que los Estados miembros habían exhortado a que se elaborara una convención internacional sobre la materia.”*

Compilando los aportes de varios autores que han contribuido al estudio y la comprensión del ciberdelito sobre las consideraciones éticas sobre el ciberdelito son fundamentales para garantizar que las acciones tomadas para prevenir y combatir este fenómeno sean justas, equitativas y respeten los derechos y la dignidad de todas las personas involucradas.

El ciberdelito en Colombia genera una serie de problemas que afectan a las entidades de orden gubernamental, empresas privadas y la sociedad en general. Los delitos cometidos a través de Internet, es un trabajo de riguroso análisis jurídico y fenomenológico que examina una a una las distintas manifestaciones delictivas, que pueden tener lugar en el medio global de interconexión por excelencia denominado Internet. Las diferentes actuaciones lesivas, sus causas, medios de ejecución, medidas preventivas y ante todo las posibilidades de subsunción en los diferentes tipos penales son objeto de un cuidadoso análisis, que con frecuencia se complementa con propuestas de mejora legislativa.

Así mismo, se examinan con detalle los diferentes fraudes susceptibles de ejecución a través de este medio y las posibilidades de recurrir, para hacer frente a los mismos, a los tipos de estafa común y estafa informática; el desarrollo exponencial y posibilidades de difusión de elementos de pornografía infantil a través de Internet y su respuesta legal; las manifestaciones lesivas de los derechos de autor, que han encontrado en este medio una

excepcional vía de desarrollo; la puerta abierta que el mismo supone a los ataques contra la intimidad y el llamado secreto de las comunicaciones; las conductas de bloqueo, difusión masiva de virus, etc. y su posible reconducción al denominado delito de daños informáticos; en definitiva, todas las manifestaciones relevantes lesivas, que son conocidas en el estado de desarrollo actual de dicho canal.

El avance vertiginoso de la tecnología digital ha dado lugar a una nueva frontera delictiva: el ciberdelito. Este fenómeno, caracterizado por la comisión de actos criminales a través de medios electrónicos y redes informáticas, presenta una serie de desafíos y complejidades que desafían las concepciones tradicionales de la justicia penal. Esto con el fin de proporcionar una visión comprensiva y estructurada de esta compleja problemática, se procederá a clasificar las distintas categorías de ciberdelitos, jerarquizar las amenazas según su impacto y frecuencia, seleccionar casos representativos para el análisis detallado y, finalmente, ordenar el contenido de manera lógica. Este método secuencial permitirá un análisis y comprensión más profundos del ciberdelito y su impacto en la sociedad moderna.

El escenario de estudio donde se adelantan los ciberataques es en una entidad de orden nacional conocida como la fiscalía general de la nación de Colombia, la cual diariamente recibe un sin número de ataques cibernéticos; El ataque, perpetrado por un grupo de ciberdelincuentes con habilidades sofisticadas, no solo causa pérdidas significativas en la información de tipo penal, sino que también socava la confianza de los ciudadanos en la seguridad de las transacciones en línea. Este escenario puede variar ampliamente y puede incluir una serie de elementos y actores, tanto en el mundo virtual como en el mundo físico.

Importancia del Tema***:*** en este artículo, se examinan los aspectos claves del ciberdelito, sus implicaciones y las estrategias para mitigar sus efectos todo esto siguiendo las experiencias vividas por muchas personas a quienes el ciberdelito les genero alguna afectación. La indagación se centra en la comprensión de los tipos específicos de ciberdelitos y sus motivaciones subyacentes. Se ha recurrido a una gama de fuentes bibliográficas, incluidos libros, artículos académicos y estudios de casos recientes, para contextualizar y respaldar este escrito. Esto incluye el análisis de nuevas tecnologías, tácticas de ataque innovadoras y cambios en el panorama de las amenazas cibernéticas.

Modalidades y modos de ciberataques en Colombia.

Los inconvenientes en la ciberseguridad radican en que los bandos atacantes no pueden ser identificados porque esto puede involucrar conflictos entre gobiernos, partidos políticos, gremios, etc. Debido a que el ciberespacio no está establecido por un país en particular, la ciberseguridad no discrimina ni tiene fronteras, por lo que se ha convertido en un tema global.

Con la expedición de la Ley 1273 de 2009, se creó el bien jurídicamente tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. De esta manera, y a efectos de sancionar las infracciones contra la confidencialidad, la integridad y la disponibilidad del mencionado bien, se tipificaron las conductas asociadas bajo los 9 delitos que se describen a continuación (Legislación Colombiana).

Artículos Ley	Tipificación.	Modalidad.	Modo.

1273/2009			
269 A	*Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá…	Acceso Físico (desde el equipo o terminal directamente afectado). Acceso Remoto.	Ingeniería Social. Software Malicioso. Phishing. Vishing. Smishing. SIM SWAP. Explotación de Vulnerabilidades.
269 B	*Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.	Impedir (Supone la inutilización absoluta del sistema, los datos o la red de telecomunicaciones). Obstaculizar (Supone la inutilización parcial del sistema, los datos o la red de Telecomunicaciones).	Ransomware de bloqueo o de cifrado. Ataque DoS. Ataque DDoS. Botnet. Ataque DNS. Buffer Overflow.
269 C	*Interceptación de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones Electromagnéticas provenientes de un sistema informático que los trasporte.	Interceptación de datos personales (sensibles, privados o semiprivados) o impersonales (Aquellos no referidos a personas pero que no resultan anónimos).	Se realiza por medios electrónicos, informáticos, ópticos, magnéticos. Trojanos (Banker). Ataque MitB Man in the browser. Ataque MitM Man in the middle.
269 D	*Uso de software malicioso.* El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional	Desarrollo de software malicioso. Uso de software malicioso.	Software Malicioso.

	software malicioso u otros programas de computación de efectos dañinos.	Distribución de software malicioso.	

Dentro de las tipologías de delitos informáticos identificadas en Colombia se encuentra el "PHISHING". Este es un programa malicioso que se infiltra en las bases de datos, extrayendo información sin dejar rastro y borrando registros de los procesos judiciales de personas bajo investigación penal. Evidenciando lo anterior surge la pregunta de investigación ¿Cuáles son las estrategias más efectivas para prevenir y mitigar el robo de información de bases de datos en entornos judiciales? Dando respuesta a la citada pregunta se deben considerar los factores como la seguridad de la red, la capacitación del personal y las medidas de protección de datos, esto con el fin de poder contrarrestar el robo de información de la cual está siendo objeto la fiscalía general de Colombia.

Estrategias para tratar de mitigar el ataque de la ciberdelincuencia en Colombia.

Para mitigar los ataques de la ciberdelincuencia, es esencial implementar una combinación de estrategias técnicas, organizacionales y legales que coadyuven al desarrollo de la ciberseguridad en las instituciones Gubernativas para ello contaríamos con:

Actualización y Parches de Software: Esto nos ayudaría a mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas. De igual manera los Firewalls y Sistemas de Detección de Intrusos (IDS) esta estrategia de implementar y configurar adecuadamente firewalls y sistemas de detección y prevención de intrusos para monitorear y bloquear actividades sospechosas. También seria de suma importancia el Cifrado de Datos, lo cual nos brindaría unas técnicas de cifrado para proteger la información tanto en tránsito como en reposo, asegurando que los datos no puedan ser leídos por terceros no autorizados.

Además, la implementación de Políticas de Seguridad que ayuden a desarrollar e implementar políticas de seguridad claras y específicas que regulen el uso de los recursos tecnológicos y la información sensible; se debe establecer un plan de respuesta a incidentes que detalle los pasos a seguir en caso de un ciberataque, incluyendo roles y responsabilidades específicos. Por otra parte, se debe dar el cumplimiento normativo ya que se debe asegurar el cumplimiento de las leyes y regulaciones aplicables relacionadas con la protección de datos y la ciberseguridad esto se logra promoviendo el desarrollo y fortalecimiento de la legislación específica contra los ciberdelitos, asegurando que las leyes estén actualizadas con las últimas tendencias y técnicas utilizadas por los delincuentes. Implementando las anteriores estrategias de seguridad informática dentro de las organizaciones o instituciones, se puede fortalecer significativamente su postura de seguridad y disminuir tanto la probabilidad como el impacto de los ataques cibernéticos.

Retos y Desafíos.

A pesar del marco legal existente, Colombia enfrenta desafíos significativos en la aplicación efectiva de estas normas, estos desafíos son:

- La rápida evolución de la tecnología y la sofisticación de los ciberataques.
- La necesidad de actualización constante de la legislación.

- El fortalecimiento de capacidades técnicas y humanas en las entidades encargadas de la ciberseguridad.
- La concientización y educación de la ciudadanía en temas de ciberseguridad.

Por lo tanto, la dimensión jurídica del ciberdelito en Colombia está conformada por un marco legislativo robusto, la participación de diversas instituciones y entidades, y la colaboración internacional, pero también requiere un continuo fortalecimiento y adaptación a los cambios tecnológicos y las nuevas modalidades de cibercrimen.

CONCLUSIONES.

Como conclusiones tenemos, la creciente preocupación por la ciberseguridad en ambos ámbitos, como lo es las instituciones estatales y las instituciones privadas, lo que ha llevado a una urgente necesidad de implementar medidas efectivas. Estas medidas son clave para salvaguardar los sistemas, datos e información de las organizaciones ante las crecientes amenazas y ataques cibernéticos. Estos ataques representan un riesgo considerable para la continuidad de las operaciones de cualquier entidad. Encuestas recientes han evidenciado el impacto significativo que los ciberataques tienen en la ejecución de actividades y la disponibilidad de información, afectando directamente la productividad y generando costos considerables de recuperación para las organizaciones afectadas.

La gestión de riesgos en seguridad informática desempeña un papel crucial en la prevención y mitigación de posibles incidentes de seguridad. Establecer políticas claras, implementar medidas de seguridad efectivas y disponer de planes de contingencia y recuperación son aspectos esenciales para reducir el impacto de los ciberataques y agilizar la restauración de las operaciones. Es imperativo asignar un presupuesto adecuado para la adquisición y mantenimiento de tecnologías de protección de la información, como licencias actualizadas y renovadas. Las organizaciones que realizan inversiones en este tipo de tecnologías tienen una mayor capacidad para salvaguardar sus sistemas y datos, lo que dificulta en gran medida su vulnerabilidad ante posibles amenazas.

La protección de la información, la mitigación de riesgos, el cumplimiento normativo y la reducción del impacto financiero son aspectos cruciales que respaldan cómo la adopción de la gestión de riesgos en seguridad informática genera ventajas significativas en Colombia. Vemos también, la Importancia de la seguridad cibernética: Destaca la importancia de contar con medidas sólidas de seguridad cibernética en instituciones gubernamentales como la fiscalía general de Colombia. Los ciberataques representan una amenaza constante y deben abordarse con seriedad para proteger los datos y garantizar el funcionamiento eficiente de las operaciones.

LIMITACIONES Y ESTUDIOS FUTUROS

La ciberdelincuencia: análisis de tendencias y estrategias de mitigación, caso Colombia; la elaboración del presente documento, estuvo circunscrito a la revisión bibliográfica, el motivo fundamental se debió a la falta de recursos económicos y el factor tiempo. El autor del trabajo se compromete a presentar un proyecto de investigación para que se apruebe, con ello disponer de recursos humanos, materiales y económicos para llevar a cabo la investigación de campo.

RECONOCIMIENTO

El autor expresa su gratitud a los miembros de la fiscalía general de la Nación de Colombia, por aportar con ideas conducentes a la cristalización del presente trabajo.

REFERENCIAS BIBLIOGRÁFICAS.

Agustina, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad: ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? Estudios Penales Y Criminológicos, 41, 705-777 Recuperado en: https://doi.org/10.15304/epc.41.7433 (15 de abril de 2024)

Antonio Rodríguez, J., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. URVIO - Revista Latinoamericana de Seguridad Ciudadana, 20, 63–79. Recuperado en: https://doi.org/10.17141/urvio.20.2017.2583 (22 de abril de 2024)

Barry C. Feld. (2017). The Evolution of the Juvenile Court : Race, Politics, and the Criminalizing of Juvenile Justice. NYU Press. Recuperado en: https://web.p.ebscohost.com/ehost/detail/detail?vid=2&sid=e5d42a97-d3ba-4c28-b7d6-5706e6f914bc%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl# (22 de abril de 2024)

Castañeda Pérez, M. S. (2022). Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022. Castañeda Pérez, M. S. (2022). Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022. Recuperado en: http://repository.unipiloto.edu.co/handle/20.500.12277/12279 (10 de mayo de 2024)

Cedeño Villacís R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista Tecnológica Ciencia Y Educación Edwards Deming, 6 (1). Recuperado en: https://doi.org/10.37957/rfd.v6i1.88 (20 de abril de 2024)

Cedeño Villacís R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista Tecnológica Ciencia Y Educación Edwards Deming, 6 (1). Recuperado en: https://doi.org/10.37957/rfd.v6i1.88 (20 de abril de 2024)

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (Pag. 149-150). Recuperado en: https://doi.org/10.17141/urvio.20.2017.2563 (20 de abril de 2024)

Maya, R. P. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Nuevo Foro Penal/Nuevo Foro Penal, 72-112. Recuperado en: https://doi.org/10.17230/nfp.13.88.3 (12 de abril de 2024)

Ortega, J. A. S., & Ortega, J. A. (2023b). I Curso de Suficiencia Profesional: Una experiencia al Derecho. En Fondo Editorial de la Universidad Privada Norbert Wiener eBooks. Recuperado en: https://doi.org/10.37768/unw.vri-cdcp.0012 (19 de abril de 2024)

Palazzi, P. A. (2006). Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 2, 61–94. Recuperado en: https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=26997447&lang=es&site=ehost-live (22 de abril de 2024)

Mayer Lux, Laura. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis, 24(1), 159-206. Recuperado el 14 de mayo de 2024 en https://dx.doi.org/10.4067/S0718-00122018000100159

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. Ius Et Praxis, 53(053), 95-110. Recuperado el 10 de mayo de 2024, en: https://doi.org/10.26439/iusetpraxis2021.n053.4995