DOI: https://doi.org/10.56712/latam.v5i4.2437

Análisis documental: impacto de la seguridad jurídica antes los delitos informáticos

Documentary analysis: impact of legal security in computer crime

Astrith Iliana Cuenca Gonzaga
acuencag@unemi.edu.ec
https://orcid.org/0009-0003-9213-4021
Universidad Estatal de Milagro
Milagro – Ecuador

Juri Evelyn Núñez Portilla
jnunezp2@unemi.edu.ec
https://orcid.org/0000-0001-5161-9186
Universidad Estatal de Milagro
Milagro – Ecuador

Artículo recibido: 12 de julio de 2024. Aceptado para publicación: 27 de julio de 2024.
Conflictos de Interés: Ninguno que declarar.

Resumen

El presente artículo estaba basado a un análisis documental sobre los delitos informáticos y el impacto en la seguridad jurídica; el delito informático o ciberdelito es cualquier comportamiento ilegal y delictivo que se da por sentado canal informático o aquellos diseñados para perturbar y dañar ordenadores o soportes electrónicos y redes de Internet. Este estudio muestra la necesidad de una mayor educación y concientización sobre la importancia de la seguridad informática en Ecuador y resalta la importancia de que las personas y organizaciones tomen medidas preventivas para protegerse de los delitos informáticos. Esta investigación proporciona información valiosa que puede ayudar a prevenir el ciberdelito. Para el desarrollo de este trabajo se incluye una descripción cuantitativa de los tipos de delitos informáticos cometidos desde los años 2018 hasta 2021. De la comparación y análisis de la información realizada durante esta investigación se puede observar que, aplicando los métodos de recolección de datos e investigación, se ha propuesto información básica para identificar los delitos informáticos más comunes.

Palabras clave: seguridad jurídica, delito informático, ciberdelito, internet

Abstract

This article was based on a documentary analysis of computer crimes and the impact on legal security; Computer crime or cybercrime is any illegal and criminal behavior that is taken for granted computer channel or those designed to disrupt and damage computers or electronic media and Internet networks. This study shows the need for greater education and awareness about the importance of computer security in Ecuador and highlights the importance of people and organizations taking preventive measures to protect themselves from computer crimes. This research provides valuable information that can help prevent cybercrime. For the development of this work, a quantitative description of the types of computer crimes committed from the years 2018 to 2021 is included. From the comparison and analysis of the information carried out during this investigation, it can be observed that, applying the data collection methods and research, basic information has been proposed to identify the most common computer crimes.

Keywords: legal security, computer crime, cybercrime, internet

Todo el contenido de LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, publicados en este sitio está disponibles bajo Licencia Creative Commons . (cc) BY

Cómo citar: Cuenca Gonzaga, A. I., & Núñez Portilla, J. E. (2024). Análisis documental: impacto de la seguridad jurídica antes los delitos informáticos. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 5 (4), 2541 – 2551. https://doi.org/10.56712/latam.v5i4.2437*

INTRODUCCIÓN

En la era digital, la seguridad jurídica se ha convertido en un pilar fundamental para garantizar la estabilidad y confianza en el uso de las tecnologías de la información y la comunicación. La proliferación de delitos informáticos, tales como el hacking, el fraude cibernético, el robo de identidad y el ciberacoso, ha puesto de manifiesto la necesidad de un marco legal robusto que pueda enfrentar estos desafíos contemporáneos. La seguridad jurídica, entendida como la certeza y previsibilidad del ordenamiento jurídico, es esencial para proteger los derechos y libertades de los individuos, así como para promover un entorno seguro y confiable para las transacciones electrónicas y el intercambio de información. (Ronquillo Barzola, 2022)

Los delitos informáticos representan una amenaza significativa no solo para la seguridad personal y la privacidad de los usuarios, sino también para la integridad de las instituciones públicas y privadas. La capacidad de los sistemas legales para adaptarse a estos nuevos tipos de delitos es crucial para mantener la confianza de la sociedad en el uso de tecnologías digitales. La falta de seguridad jurídica en el ámbito cibernético puede llevar a una percepción de impunidad, incentivando la comisión de delitos y desincentivando la inversión y la innovación en tecnologías emergentes. (Caycho Pinchi & Saguma Rivera, 2021)

Uno de los medios más comunes para cometer tales delitos es Internet, ya que permite a muchas personas en todo el mundo conectarse y comunicarse y también brinda oportunidades que permiten a quienes cometen delitos esconderse detrás de una pantalla y operar. Salió, realizó sus acciones sin ser registrado y en algunos casos, no era quien decía ser, cometiendo delitos varias veces sin ningún delito físico y sin pruebas que lo demostraran. Debido a esto, este tipo de delitos son difíciles de probar y muchas víctimas prefieren no denunciarlos antes que ser castigadas porque saben que están siendo atacadas por estos delincuentes.

Al comprender la seguridad jurídica, no se debe perder de vista su otra importancia para el Derecho penal, que radica en configurar, definir mediante otras garantías, las condiciones para la punibilidad de una conducta en un ámbito que se puede clasificar como protector utilitario. Si el proceso de configuración de dicha conducta desde el punto de vista de su utilidad jurídica no se refleja adecuadamente en las normas y procedimientos que prescriben su prevención y persecución, se generarían una situación contraria al principio de tipicidad, lo que nos llevaría a una situación de inseguridad jurídica. De esta manera, se cierra lógicamente el ciclo, ya que en el impulso preventivo (cuyo marco teórico también correspondería a la Política criminal) la seguridad jurídica, en su doble función de garantía contra el poder punitivo del Estado y como configuradora de dicho poder, debe contribuir a minimizar la probabilidad de daño, en este caso penal, que es precisamente el objetivo del régimen preventivo. (Moreyra Saldaña, 2024)

Este artículo examina el impacto de la seguridad jurídica en la prevención y persecución de delitos informáticos, analizando cómo los marcos legales actuales abordan estos desafíos y qué mejoras son necesarias para fortalecer la respuesta jurídica ante la creciente sofisticación de las amenazas cibernéticas. Asimismo, se explorará el papel de la cooperación internacional y la implementación de políticas públicas eficaces para garantizar un entorno digital seguro y protegido. A través de un análisis exhaustivo, se busca destacar la importancia de la seguridad jurídica como elemento clave para la protección y el desarrollo sostenido en la era digital.

DESARROLLO

Seguridad Jurídica

La seguridad jurídica es un principio fundamental del derecho que garantiza a los ciudadanos la certeza y previsibilidad del ordenamiento jurídico en sus relaciones y actuaciones. Este principio implica que las leyes y normas sean claras, públicas, estables y aplicadas de manera consistente, de modo que las personas puedan saber con anticipación cuáles son sus derechos y obligaciones y prever las consecuencias legales de sus acciones. (Rodríguez Cardo, 2024)

Según (Monereo Pérez, 2022) expresa que Hans Kelsen, uno de los más influyentes teóricos del derecho, define la seguridad jurídica como un principio del ordenamiento jurídico que garantiza la previsibilidad del derecho. La seguridad jurídica se logra cuando las normas jurídicas son claras, precisas y estables, permitiendo a los ciudadanos prever las consecuencias legales de sus acciones. Por lo que es esencial la seguridad jurídica para la validez del derecho positivo, ya que asegura que las normas sean aplicadas de manera uniforme y no arbitraria.

Por otra parte, Norberto Bobbio, un destacado filósofo del derecho, considera la seguridad jurídica como uno de los valores fundamentales del ordenamiento jurídico, sostiene que la seguridad jurídica implica la certeza de las normas, su publicidad y su estabilidad en el tiempo. Asimismo, destaca que la seguridad jurídica es fundamental para la libertad individual, ya que permite a las personas conocer sus derechos y obligaciones y prever las consecuencias de sus actos. (Iñiguez Ortiz, 2020)

Karl Larenz, un renombrado jurista alemán, define la seguridad jurídica como la garantía de que las leyes serán aplicadas de manera consistente y predecible, subraya la importancia de la estabilidad normativa y la coherencia en la interpretación y aplicación de las normas. La seguridad jurídica no solo protege a los individuos contra cambios arbitrarios en la legislación, sino que también fomenta la confianza en el sistema legal. (Cardo & Murcia, 2024)

La seguridad jurídica, según estos autores, es un principio fundamental del derecho que garantiza la claridad, estabilidad y previsibilidad del ordenamiento jurídico. Esto permite a los ciudadanos conocer sus derechos y obligaciones, actuar con confianza y prever las consecuencias legales de sus acciones. La seguridad jurídica es esencial para la justicia, la libertad individual y el funcionamiento ordenado de la sociedad.

Delitos Informático

El delito informático es un acto ilícito que se comete utilizando tecnologías de la información y la comunicación (TIC), como computadoras, redes de computadoras, internet y dispositivos electrónicos. Estos delitos pueden variar en su naturaleza y objetivos, afectando a individuos, empresas y gobiernos, y pueden tener consecuencias significativas para la seguridad, privacidad y estabilidad económica y social. (Rodríguez et al.2023)

Julio Téllez Valdés, experto en derecho informático, define los delitos informáticos como aquellas conductas ilícitas que se cometen utilizando tecnologías de la información y la comunicación, afectando la confidencialidad, integridad, disponibilidad de los datos y sistemas informáticos, acentúa que los delitos informáticos no solo incluyen el acceso no autorizado a sistemas, sino también el fraude, el robo de identidad, y la difusión de virus informáticos. (Ormaza & Ycaza, 2023)

En el libro "The Law of Cybercrimes and Their Investigations" de George Curtis, se define el delito informático como cualquier actividad delictiva que implique una computadora, una red de computadoras o un dispositivo en red. Estos autores explican que los delitos informáticos abarcan una amplia gama de actividades ilegales, desde el hacking y el phishing hasta la distribución de malware y

el ciberacoso, destacando la evolución constante de las técnicas y métodos utilizados por los ciberdelincuentes. (Curtis George, 2011)

Por su parte (García Méndez, 2017) especialista en derecho penal, define los delitos informáticos como acciones delictivas que se perpetran mediante el uso de sistemas informáticos o redes de comunicación electrónica, resalta la importancia de adaptar el marco legal a las nuevas realidades tecnológicas, dado que estos delitos pueden tener un impacto significativo en la privacidad, la seguridad y la economía.

Los delitos informáticos comprenden una amplia gama de actividades ilícitas que involucran el uso de tecnologías digitales. Estas conductas afectan la seguridad, privacidad y la integridad de los sistemas y datos informáticos, presentando desafíos únicos para la legislación y la aplicación de la ley. La necesidad de marcos legales adaptativos, cooperación internacional y técnicas avanzadas de investigación es fundamental para abordar eficazmente los delitos informáticos en el contexto global actual.

Ataques Informáticos

Los ataques informáticos son acciones maliciosas dirigidas a sistemas, redes o dispositivos informáticos con el objetivo de causar daños, robar información, obtener acceso no autorizado o interrumpir el funcionamiento normal de los servicios. Estos ataques representan una amenaza significativa para la seguridad y la integridad de los sistemas y datos en el mundo digital. Comprender los diferentes tipos de ataques y sus características es fundamental para desarrollar estrategias de defensa efectivas y proteger los activos de información. Las organizaciones y los individuos deben estar continuamente informados y preparados para enfrentar estas amenazas mediante la implementación de medidas de seguridad robustas y actualizadas. (Ribera et al.2022)

(Stallings William, 2017) en su libro "Cryptography and Network Security: Principles and Practice", define los ataques informáticos como acciones deliberadas que tienen como objetivo comprometer la seguridad de la información y los sistemas de comunicación, destaca que estos ataques pueden ser pasivos, como la interceptación de datos, o activos, como la modificación de los datos o el sabotaje de sistemas.

Por otra parte, (Bruce Schneier,2017) expresa los ataques informáticos como cualquier acción intencional que busca explotar vulnerabilidades en un sistema informático con fines maliciosos, señala que estos ataques pueden variar desde el robo de información hasta la interrupción de servicios, y subraya la importancia de una estrategia de defensa en profundidad para protegerse contra ellos.

Los ataques informáticos son acciones maliciosas intencionales que buscan explotar vulnerabilidades en los sistemas de información y comunicación para obtener acceso no autorizado, robar datos, interrumpir servicios o causar daños. Expertos como William Stallings y Bruce Schneier han destacado la diversidad de métodos y objetivos de estos ataques, así como la necesidad de implementar medidas de seguridad robustas para mitigar sus efectos. La comprensión y la preparación ante estas amenazas son esenciales en el entorno digital actual, donde la ciberseguridad se ha convertido en una prioridad crítica para individuos, organizaciones y estados.

Tipos y Modalidades de Delitos Informáticos

Los delitos informáticos abarcan una amplia gama de actividades ilícitas realizadas a través de tecnologías de la información y comunicación, comprender los diferentes tipos y formas de estos delitos es esencial para implementar medidas de seguridad efectivas y protegerse contra posibles ataques. La colaboración internacional y la actualización constante de las leyes y tecnologías de seguridad son cruciales para combatir eficazmente estos delitos.

- Acceso no Autorizado (Hacking)
- Intercepción de Comunicaciones (Sniffing)
- Daños o Alteración de Datos (Data Diddling)
- Fraude Informático
- Phishing
- Distribución de Malware
- Robo de Identidad
- Modalidades de Delitos Informáticos
- Ciberterrorismo
- Ciberespionaje
- Ciberacoso
- Fraude Electrónico
- Sabotaje Informático
- Estafas en Línea

Las modalidades de delitos informáticos son variadas y complejas, reflejando la evolución constante de la tecnología y la creatividad de los delincuentes. Entender estas modalidades es crucial para desarrollar estrategias de prevención y defensa efectivas, y para crear un entorno digital seguro tanto para individuos como para organizaciones.

METODOLOGÍA

Dada la naturaleza cualitativa este estudio fue realizado por medio de la investigación descriptiva – analítica acudiendo a la revisión documental de los diversos ataques denunciados en Ecuador en los últimos años, lo cual permitió la obtención de información de diferentes fuentes digitales. Este trabajo investigativo está encaminado al estudio de la seguridad jurídica ante los delitos informáticos más frecuentes en Ecuador.

RESULTADOS Y DISCUSIÓN

Tabla 1

Cantidad de denuncias sobre delitos informáticos en Ecuador

Art. COIP	Tipos delitos	2018	2019	2020	2021
212	Suplantación de identidad	4180	4607	2162	222
328	Falsificación y uso de documentos falsos	3292	3231	1448	1574
190	Apropiación fraudulenta por medios electrónicos	1451	1746	1033	3962
234	Acceso no concedido a un sistema informático, telemático o de telecomunicaciones	236	246	175	274
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	202	166	85	152
232	Ataques a la integridad de sistemas informáticos	87	113	51	86
230	Intercepción ilegal de datos	41	87	45	35
231	Transferencia electrónica de activos patrimonial	38	49	31	170
229	Revelación ilegal de base de datos	44	34	18	23
	Total	9571	10279	5048	6498

Fuente: Yomar Toala, Indio (2021) https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf. Revista Científica de Ciencias Jurídicas, Criminología y Seguridad (2021) https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf,

https://www.primicias.ec/noticias/seguridad/ciberdelitos-ecuador-estafas-analfabetos-digitales vulnerables/#:~:text=En%202021%20se%20registraron%20851,2022%3B%20y%2098%20en%202023.

Analizando las denuncias sobre delitos informáticos en Ecuador desde 2018 hasta el 2021, se puede expresar que hubo un incremento del 10.2% en los casos de suplantación de identidad de 2018 a 2019, pasando de 4180 a 4607 casos. En el 2020, los casos se redujeron drásticamente a 2162, una disminución del 53.1% en comparación con el 2019. Esta caída puede ser atribuida a diversas razones, como la implementación de medidas de seguridad más estrictas o cambios en las actividades delictivas debido a la pandemia de COVID-19. En el 2021, los casos cayeron aún más, llegando a solo 222, lo que representa una disminución del 89.7% respecto al año anterior. Esta notable reducción podría indicar una mejora significativa en las medidas de prevención y detección de suplantación de identidad o un cambio en la tendencia de los delincuentes hacia otros tipos de delitos. El análisis de estos datos muestra una tendencia general a la baja en los casos de suplantación de identidad desde 2019. La disminución más significativa se observó en 2020 y 2021, lo que sugiere que se han implementado medidas efectivas para combatir este delito o que ha habido un cambio en el enfoque de los delincuentes hacia otras actividades delictivas.

Los casos de falsificación y uso de documentos falsos disminuyeron levemente de 3292 en 2018 a 3231 en 2019, una reducción del 1.9%. Esto indica una estabilización en la ocurrencia de este delito durante este período. En 2020, los casos se redujeron drásticamente a 1448, una disminución del 55.2% en comparación con 2019. Este descenso significativo podría estar relacionado con factores externos, como la pandemia de COVID-19, que podría haber alterado las oportunidades para cometer este tipo de delitos. En 2021, los casos aumentaron ligeramente a 1574, un incremento del 8.7% en comparación con 2020. Este pequeño repunte podría reflejar un retorno gradual a las actividades normales y, por ende, más oportunidades para cometer falsificaciones. Los datos muestran una tendencia general a la baja en los casos de falsificación y uso de documentos falsos desde 2018, con un notable descenso en 2020, posiblemente debido a la pandemia. El ligero aumento en 2021 sugiere un posible retorno a patrones anteriores a la pandemia, aunque el número de casos sigue siendo significativamente menor que en 2018 y 2019.

Por otra parte, la apropiación Fraudulenta por Medios Electrónicos los casos aumentaron de 1451 en 2018 a 1746 en 2019, un incremento del 20.4%. Este incremento moderado podría indicar una creciente tendencia hacia la comisión de este tipo de delito. En 2020, los casos disminuyeron significativamente a 1033, una reducción del 40.8%. Esta caída notable puede estar asociada a la pandemia de COVID-19, que pudo haber alterado las dinámicas del delito. En 2021, los casos se dispararon a 3962, un aumento del 283.7% en comparación con 2020. Este incremento abrupto podría reflejar un cambio en las tácticas de los delincuentes o un aumento en la vulnerabilidad de los sistemas electrónicos debido al incremento de actividades en línea durante la pandemia. Los datos muestran una tendencia variable con un notable aumento en 2021. Este incremento podría ser resultado de factores como el aumento de transacciones electrónicas y la vulnerabilidad de los sistemas durante la pandemia. La marcada variabilidad subraya la necesidad de mejorar las medidas de seguridad y vigilancia en el ámbito de las transacciones electrónicas.

Las denuncias por Acceso No Concedido a un Sistema Informático, Telemático o de Telecomunicaciones hubo un pequeño aumento en los casos de 236 en 2018 a 246 en 2019, un incremento del 4.2%. Esto sugiere una estabilidad en la ocurrencia de este delito durante este período. En 2020, los casos se redujeron a 175, una disminución del 28.9% en comparación con 2019. Este descenso podría estar asociado con cambios en las actividades delictivas durante la pandemia de COVID-19 o con mejoras en las medidas de seguridad cibernética. En 2021, los casos aumentaron significativamente a 274, un incremento del 56.6% respecto al año anterior. Este aumento puede indicar un resurgimiento en las actividades delictivas relacionadas con el acceso no autorizado a sistemas

informáticos, posiblemente debido a la mayor dependencia de la tecnología durante y después de la pandemia.

Los casos de Contacto con Finalidad Sexual con Menores de Dieciocho Años por Medios Electrónicos disminuyeron de 202 en 2018 a 166 en 2019, una reducción del 17.8%. Esto sugiere una posible efectividad en las medidas de prevención o una disminución en la incidencia de este delito. En 2020, los casos se redujeron drásticamente a 85, una disminución del 48.8% en comparación con 2019. Este descenso significativo puede estar relacionado con las restricciones y cambios en la interacción social durante la pandemia de COVID-19. En 2021, los casos aumentaron a 152, un incremento del 78.8% respecto al año anterior. Lo que puede indicar un resurgimiento de las actividades delictivas relacionadas con el contacto sexual con menores a medida que se relajaron las restricciones de la pandemia y la gente volvió a utilizar más los medios electrónicos para interactuar.

Los ataques a la Integridad de Sistemas Informáticos aumentaron de 87 en 2018 a 113 en 2019, un incremento del 29.9%. Esto indica un aumento en la incidencia de ataques a la integridad de los sistemas informáticos durante este período. En 2020, los casos se redujeron drásticamente a 51, una disminución del 54.9% en comparación con 2019. Esta caída significativa puede estar asociada con la pandemia de COVID-19, que pudo haber cambiado las oportunidades y métodos de los atacantes. En 2021, los casos aumentaron nuevamente a 86, un incremento del 68.6% respecto al año anterior. Este aumento sugiere una posible recuperación de las actividades delictivas relacionadas con ataques a la integridad de sistemas, posiblemente debido a la reanudación de actividades normales y el mayor uso de sistemas informáticos. Los datos muestran fluctuaciones en los casos de ataques a la integridad de sistemas informáticos. Hubo un incremento de 2018 a 2019, seguido por una significativa reducción en 2020, probablemente debido a la pandemia. Sin embargo, en 2021 se observó una recuperación en los casos, lo que indica un resurgimiento en este tipo de actividades delictivas.

Los casos aumentaron de 41 en 2018 a 87 en 2019, un incremento del 112%. Este aumento significativo indica un crecimiento en la incidencia de intercepción ilegal de datos durante este período, posiblemente debido a un aumento en la actividad delictiva o a una mayor detección de estos casos. En 2020, los casos se redujeron drásticamente a 45, una disminución del 48.3% en comparación con 2019. Esta reducción significativa puede estar relacionada con la pandemia de COVID-19, que afectó las actividades normales y pudo haber reducido las oportunidades para cometer este tipo de delitos. En 2021, los casos disminuyeron aún más a 35, una reducción del 22.2% respecto al año anterior. Esta disminución continuada sugiere una posible tendencia a la baja en la intercepción ilegal de datos, quizás debido a mejoras en las medidas de seguridad y la concienciación sobre estos delitos. Los datos muestran una tendencia inicial al alza en los casos de intercepción ilegal de datos de 2018 a 2019, seguida de una notable disminución en 2020 y una reducción adicional en 2021. Este patrón podría reflejar cambios en las oportunidades y métodos de los delincuentes, influenciados por factores como la pandemia y las mejoras en la ciberseguridad.

Las transferencias Electrónica de Activos Patrimonial estos casos aumentaron de 38 en 2018 a 49 en 2019, un incremento del 28.9%. Este aumento sugiere un ligero crecimiento en la incidencia de este tipo de delito durante este período. En 2020, los casos disminuyeron a 31, una reducción del 36.7% en comparación con 2019. Este descenso puede estar relacionado con los efectos de la pandemia de COVID-19, que alteró muchas actividades económicas y delictivas. En 2021, los casos aumentaron drásticamente a 170, un incremento del 448.4% respecto al año anterior. Este aumento significativo podría estar relacionado con un mayor uso de las tecnologías de transferencia electrónica durante y después de la pandemia, así como con una mayor explotación de vulnerabilidades por parte de los delincuentes. Los datos muestran una fluctuación en los casos de transferencia electrónica de activos patrimoniales con un ligero aumento inicial seguido de una disminución en 2020 y un aumento exponencial en 2021. Este patrón sugiere que, mientras la pandemia inicialmente redujo las

oportunidades para este delito, el mayor uso de tecnologías electrónicas y posibles vulnerabilidades explotadas resultaron en un aumento significativo en 2021.

CONCLUSIÓN

Ecuador ha fortalecido su marco jurídico y sus capacidades institucionales para protegerse contra los delitos informáticos, aunque sigue enfrentando desafíos en un entorno digital en constante evolución, Ecuador cuenta con leyes específicas que penalizan diversos tipos de delitos informáticos, como acceso ilícito a sistemas, sabotaje informático, fraude informático, entre otros. La Ley Orgánica de Comunicación, por ejemplo, incluye disposiciones sobre la protección de datos personales y la responsabilidad por la divulgación ilegal de información.

También, Ecuador tiene normativas específicas para la protección de datos personales, reguladas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y la Superintendencia de Información y Comunicación (SUPERCOM). Estas regulaciones buscan garantizar que las empresas y entidades públicas protejan adecuadamente la información personal de los ciudadanos. Se promueven iniciativas de educación y concientización sobre seguridad digital entre la población, empresas y funcionarios públicos para prevenir delitos informáticos y mejorar la respuesta ante incidentes de ciberseguridad.

Crear un entorno jurídico sólido para combatir el delito cibernético puede ayudar a mantener la confianza en las tecnologías digitales, la conciencia sobre la seguridad en línea es esencial para la adopción y el desarrollo continuo de innovaciones tecnológicas.

REFERENCIAS

Bruce Schneier, (2017). Secrets and Lies: Digital Security in a Networked World. https://icdt.osu.edu/secrets-and-lies-digital-security-networked-world

Cardo, I. A. R. & Murcia, J. G. (2024). La Seguridad Jurídica en el Derecho del Trabajo y de la Seguridad Social¿ Un principio en decadencia?. [HTML]

Caycho Pinchi, J. C. & Saguma Rivera, D. E. (2021). Medidas de protección informática y su eficacia en la prevención del delito de suplantación de identidad cibernética en la ciudad de Trujillo http://repositorio.uprit.edu.pe/bitstream/handle/UPRIT/421/TESIS-%20CAYCHO%20PINCHI%20-%20SAGUMA%20RIVERA.pdf?sequence=1&isAllowed=y

Curtis George, (2011). "The Law of Cybercrimes and Their Investigations" https://www.routledge.com/The-Law-of-Cybercrimes-andTheirInvestigations/Curtis/p/book/9781439858318

Ecuador. Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial No. 449. Gobierno del Ecuador. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf.

Ecuador. Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento 180. Gobierno del Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

García Méndez, Emilio (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual Revista Nuevo Foro Penal Vol. 13, No. 88, enero-junio 2017, pp. 72-112. Universidad EAFIT, Medellín (ISSN 0120-8179)

Iñiguez Ortiz, A. N. (2020). La imputabilidad en los adolescentes a partir de los 16 años de edad, a fin de garantizar los derechos de la víctima y la seguridad jurídica. http://repositorio.ulvr.edu.ec/handle/44000/3817

Monereo Pérez, José Luis (2024) Sociología crítica del derecho y teoría jurídica en Hans Kelsen https://revistas.uma.es/index.php/REJLSS/article/view/15353/16787

Moreyra Saldaña, L. A. (2024). El registro de parentesco RENIEC y su incorporación a los procesos de sucesión intestada para la seguridad jurídica, Lima 2023. https://repositorio.ucv.edu.pe/handle/20.500.12692/142769

Ormaza, A. C. L. & Ycaza, J. C. P. (2023). Tipificación de la mala práctica médica en la legislación ecuatoriana: análisis comparativo. Dominio de las Ciencias. dominiodelasciencias.com

Ribera, A. J., Genovés, V. G., & Nohales, P. S. (2022). " El delincuente en busca de sentido". El papel de la dimensión existencial en la carrera delictiva. Revista Española de Investigación Criminológica, 20(1), 1-20. criminologia.net

Rodríguez Cardo, I. A. (2024). La Seguridad Jurídica en el Derecho del Trabajo y de la Seguridad https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DT-2024-327

Rodríguez, P. O. P., Andrade, G. J. S., & Inca, G. C. N. (2023). Análisis comparativo de los derechos y obligaciones de la unión de hecho en Argentina, Chile y Ecuador. Estudios Del Desarrollo Social: Cuba y América Latina, 11(Especial No. 1), 198-206. uh.cu

Ronquillo Barzola, W. M. (2022). La proporcionalidad de la pena en el delito de abigeato y la seguridad jurídica. https://dspace.uniandes.edu.ec/handle/123456789/15144

Stallings William, (2017). Cryptography and Network Security: Principles and Practice. https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf

Soler, M. C. 2.3. Precipitadores situacionales del delito69. El paso al acto en las conductas de Bullying y Cyberbullying. Interacción persona-ambiente., 186. uma.es

Toledo, P. (2021). Análisis comparativo de las leyes sobre el teletrabajo en el Cono Sur. Journal of Management & Business Studies. uautonoma.cl

Todo el contenido de **LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades**, publicados en este sitio está disponibles bajo Licencia Creative Commons (cc) BY.