Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 6.1
Edición Especial VI 2026

IMPACTO DE LOS CIBERDELITOS EN LA VIDA SOCIAL Y ACADÉMICA DE ESTUDIANTES EN ECUADOR Y LA AFECTACIÓN DE SUS DERECHOS CONSTITUCIONALES: UN ESTUDIO EN LA UNIVERSIDAD DE GUAYAQUIL

IMPACT OF CYBERCRIME ON THE SOCIAL AND ACADEMIC LIFE OF STUDENTS IN ECUADOR AND THE IMPACT ON THEIR CONSTITUTIONAL RIGHTS: A STUDY AT THE UNIVERSITY OF GUAYAQUIL

Autores: [1]Alberto Emmanuel Cárdenas Bolaños y [2]Hugo Alberto Cárdenas Echeverría.
[1]ORCID ID: https://orcid.org/0009-0002-8926-5760
[2]ORCID ID: https://orcid.org/0009-0006-7471-4921
[1]E-mail de contacto: alberto.cardenas@upacifico.edu.ec
[2]E-mail de contacto: hugo.cardenase@ug.edu.ec
Afiliación:[1]*Universidad del Pacífico, (Ecuador). [2]*Universidad de Guayaquil, (Ecuador).
Artículo recibido: 28 de Junio del 2026.
Artículo revisado: 30 de Junio del 2026.
Artículo aprobado: 30 de Junio del 2026.
[1]Abogado de los Tribunales y Juzgados de la República del Ecuador, (Ecuador). Magíster en Derecho mención Derecho Procesal. Magíster en Derecho Notarial y Registral.
[2]Licenciada en Ciencias Sociales y Políticas graduado de la Universidad de Guayaquil, (Ecuador). Abogado de los Tribunales y Juzgados de la República del Ecuador graduado de la Universidad de Guayaquil, (Ecuador). Magíster en Diseño Curricular graduado de la Universidad de Guayaquil, (Ecuador).

Resumen

El objetivo principal de esta investigación fue determinar el impacto de los ciberdelitos en las actividades académicas y sociales de los estudiantes de la Universidad de Guayaquil. El estudio abordó problemas como el robo de identidad, el ciberacoso, el ciberterrorismo y el contacto sospechoso. Se utilizó una metodología no experimental, cuantitativa, de corte transversal y tipología descriptiva y correlacional, validando el cuestionario con un índice de fiabilidad de 0.984 en el Alfa de Cronbach. La población consistió en 53,408 estudiantes, con una muestra de 382 participantes seleccionados de diferentes facultades. Los resultados muestran correlaciones significativas entre los ciberdelitos y sus efectos en el rendimiento académico y las interacciones sociales. La principal conclusión es que la exposición a ciberdelitos disminuye la participación en actividades académicas y sociales, afectando también el bienestar emocional de los estudiantes. Se recomienda a las autoridades universitarias desarrollar políticas de ciberseguridad y educación para mitigar estos riesgos y promover un entorno digital seguro para la comunidad universitaria.

Palabras clave: Ciberdelincuencia, Impacto social, Ciberseguridad, Delitos informáticos.

Abstract

The main objective of this research was to determine the impact of cybercrimes on the academic and social activities of students at the University of Guayaquil. The study addressed issues such as identity theft, cyberbullying, cyberterrorism, and suspicious contact. A non-experimental, quantitative, cross-sectional methodology and descriptive and correlational typology were used, validating the questionnaire with a reliability index of 0.984 in Cronbach's Alpha. The population consisted of 53,408 students, with a sample of 382 participants selected from different faculties. The results show significant correlations between cybercrimes and their effects on academic performance and social interactions. The main conclusion is that exposure to cybercrimes decreases participation in academic and social activities, also affecting the emotional well-being of students. University authorities are recommended to develop cybersecurity and education policies to mitigate these risks and promote a safe digital environment for the university community.

Keywords: Cybercrime, Social impact, Cybersecurity, Computer crimes.

Sumário

O principal objetivo desta pesquisa foi determinar o impacto do cibercrime nas atividades acadêmicas e sociais dos estudantes da Universidade de Guayaquil. O estudo abordou questões como roubo de identidade, cyberbullying, ciberterrorismo e atividades online suspeitas. Foi utilizada uma metodologia não experimental, quantitativa, transversal, descritiva-correlacional, validando o questionário com um coeficiente alfa de Cronbach de 0,984. A população foi composta por 53.408 estudantes, com uma amostra de 382 participantes selecionados de diferentes faculdades. Os resultados mostram correlações significativas entre o cibercrime e seus efeitos no desempenho acadêmico e nas interações sociais. A principal conclusão é que a exposição ao cibercrime diminui a participação em atividades acadêmicas e sociais, afetando também o bem-estar emocional dos estudantes. Recomenda-se que as autoridades universitárias desenvolvam políticas de cibersegurança e educação para mitigar esses riscos e promover um ambiente digital seguro para a comunidade universitária.

Palavras-chave: Cibercrime, Impacto social, Cibersegurança, Crimes informáticos.

Introducción

El espectro de los ciberdelitos comprende diversas conductas ilícitas, como el acceso no autorizado a sistemas, el fraude, la difusión de contenido ilegal y el acoso en línea. Entre estas, el acoso cibernético constituye una de las principales amenazas para la comunidad universitaria, debido a sus repercusiones sociales, psicológicas y académicas (Akhter et al., 2023). De acuerdo con Brands y Van (2022), Quirumbay et al. (2022) y Singh et al. (2022), aunque los estudiantes son víctimas de múltiples delitos informáticos, el ciberacoso requiere una atención prioritaria por su creciente incidencia. En este contexto, la presente investigación analiza la magnitud de este problema entre estudiantes de la Universidad de Guayaquil e identifica los factores que favorecen su ocurrencia. El desarrollo de las tecnologías de la información ha impulsado importantes transformaciones sociales, pero también ha facilitado la expansión de la ciberdelincuencia (Phan et al., 2021).

A nivel internacional, los ciberdelitos han evolucionado hacia modalidades más complejas y transnacionales (Wall, 2024), favorecidas por la globalización digital (AllahRakha, 2024; Sharma et al., 2023), lo que representa nuevos retos para la seguridad jurídica en Ecuador (Cuenca y Núñez, 2024). Asimismo, la percepción del riesgo y el temor a ser víctima varían según el contexto; mientras en Europa predominan las preocupaciones por los delitos económicos en línea (Cook et al., 2023), en Latinoamérica se enfatiza la vulneración de derechos como la privacidad y la integridad (Lucero, 2023). En este sentido, Griffith et al. (2023) y Guedes et al. (2023) evidencian que la victimización digital afecta el desarrollo académico y social de los jóvenes.

Diversos autores destacan la necesidad de fortalecer las estrategias legales y educativas para enfrentar este fenómeno. Yongmei y Afzal (2023) resaltan la importancia de contar con marcos normativos preventivos, mientras que Del Pezo (2023) señala que las limitaciones en el tratamiento de la evidencia digital reducen la eficacia de la respuesta judicial en Ecuador. Del mismo modo, Cuenca y Núñez (2024) sostienen que la seguridad jurídica constituye un elemento fundamental para combatir la impunidad derivada de los delitos informáticos. En Ecuador, los casos de chantaje y extorsión digital afectan principalmente a jóvenes de entre 16 y 21 años, quienes suelen ser

engañados mediante perfiles falsos en redes sociales para obtener contenido íntimo que posteriormente es utilizado como mecanismo de extorsión (Álvarez et al., 2021). Frente a esta realidad, la investigación se justifica por la necesidad de analizar el impacto de los ciberdelitos en el entorno universitario y su influencia sobre la normalidad social y educativa de los estudiantes. En consecuencia, el objetivo del estudio es establecer la relación entre la ciberdelincuencia y la experiencia universitaria, identificando patrones de incidencia y sus efectos sobre la dinámica académica y social.

Entre los objetivos específicos de esta investigación se encuentra analizar la relación entre los ciberdelitos y la normalidad social y educativa en el entorno universitario, con el propósito de aportar evidencia que favorezca el desarrollo de estrategias legales, preventivas y multidisciplinarias orientadas a reducir el impacto de la ciberdelincuencia en la comunidad estudiantil. Los estudios sobre las redes de ciberdelincuencia evidencian que estas difieren de las organizaciones criminales tradicionales. Aunque comparten ciertas características con grupos delictivos convencionales, las estructuras cibernéticas son más dinámicas, descentralizadas y adaptables, adoptando incluso modelos propios del ámbito empresarial (Nguyen y Luong, 2021).

En este escenario, predominan organizaciones distribuidas, sin liderazgos claramente definidos, donde los integrantes actúan con mayor autonomía (Rawat, 2023). Además, los foros virtuales constituyen espacios de encuentro para coordinar actividades ilícitas y generar mecanismos de confianza entre delincuentes, pese al anonimato del entorno digital (Griffith et al., 2023). Paralelamente, las redes fuera de línea continúan fortaleciendo estas organizaciones, que incorporan nuevas tecnologías y tácticas para incrementar sus beneficios económicos, siendo grupos como Cosmic Lynx, Exaggerated Lion, Fin7 y Florentine Banker algunas de las amenazas más relevantes (Ene y Imo, 2024).

La creciente sofisticación de estas organizaciones les permite operar desde jurisdicciones con menor alcance legal, combinar modalidades delictivas como ransomware y extorsión, y aprovechar escenarios como el incremento del teletrabajo y la educación virtual para ejecutar ataques mediante aplicaciones falsas, errores tipográficos y secuestro de URL dirigidos a usuarios con escasa experiencia tecnológica (Arpaci y Aslan, 2023). Asimismo, los ciberdelincuentes perfeccionan técnicas de ingeniería social, phishing y suplantación de identidad, investigando previamente a sus víctimas mediante la información disponible en redes sociales para desarrollar ataques altamente personalizados y difíciles de detectar (Pawlak et al., 2020).

Las organizaciones dedicadas al cibercrimen emplean estrategias de vigilancia prolongada para estudiar el comportamiento de sus víctimas y ejecutar ataques altamente personalizados. Mediante técnicas de ingeniería social, inducen a los usuarios a acceder a documentos o plataformas fraudulentas que les permiten obtener credenciales de acceso y controlar correos electrónicos, archivos, calendarios y contactos, facilitando posteriormente acciones como ransomware, robo de información, extorsión o fraude económico (Keenlyside et al., 2021). El ciberdelito trasciende el ámbito virtual y produce consecuencias económicas, sociales y personales, afectando derechos fundamentales como la privacidad y la seguridad. Su ocurrencia depende tanto de la

vulnerabilidad de las víctimas como de factores psicológicos y conductuales de los delincuentes, razón por la cual diversas teorías criminológicas se han adaptado para comprender el perfil de los ciberdelincuentes y fortalecer las estrategias de prevención y disuasión (Phillips et al., 2022; Chandra y Snowe, 2020).

Actualmente, la ciberdelincuencia constituye una industria internacional organizada que opera mediante mercados clandestinos en la *dark web*, donde se comercializan herramientas de ataque, datos robados y servicios ilícitos, permitiendo que incluso personas con escasos conocimientos técnicos ejecuten ciberataques (Samreena, 2020). Además, los delincuentes aprovechan avances tecnológicos como la inteligencia artificial para generar desinformación, vulnerar sistemas de seguridad y explotar el incremento del trabajo remoto y la educación virtual (Chang, 2020). Entre las modalidades más frecuentes se encuentran el fraude informático, el robo de identidad, la vulneración de la privacidad, la explotación sexual infantil y los ataques dirigidos al sector sanitario, cuya incidencia aumentó significativamente durante la pandemia de COVID-19 mediante la creación masiva de dominios y sitios web maliciosos (Ene y Imo, 2024; Jobi et al., 2024). Aunque muchas de estas conductas existían antes del entorno digital, Internet ha ampliado su alcance, velocidad e impacto, convirtiendo al cibercrimen en una evolución de la delincuencia tradicional (Choi et al., 2022).

En este contexto, los ciberdelincuentes, tanto de forma individual como en grupos organizados, utilizan tecnologías digitales para acceder a información confidencial y obtener beneficios económicos, apoyándose en mercados clandestinos especializados y en mecanismos de anonimato que dificultan su identificación. Esta realidad continúa representando un desafío para la legislación y los organismos encargados de la investigación y persecución de los delitos informáticos a nivel internacional (Drury et al., 2022). Los atacantes informáticos comprenden tanto especialistas en pruebas de seguridad como ciberdelincuentes que explotan vulnerabilidades con fines económicos o maliciosos. Estos últimos operan de forma independiente o integran organizaciones criminales que comercializan herramientas de ataque, códigos maliciosos, servicios de botnets y datos robados, conformando un mercado ilícito altamente especializado (Monteith et al., 2021).

Las tecnologías de Internet han fortalecido las redes de ciberdelincuencia al eliminar las barreras geográficas y facilitar la comunicación entre delincuentes mediante foros especializados, donde intercambian información, conocimientos y recursos para ejecutar ataques con mayor eficacia (Guerra et al., 2021). En consecuencia, la participación en actividades delictivas ya no depende exclusivamente de conocimientos técnicos avanzados, pues las organizaciones pueden contratar expertos o adquirir servicios especializados. Además, la exposición a ciberataques incrementa la percepción de inseguridad, el estrés y el temor de la población, generando repercusiones sociales y psicológicas significativas (Kozik et al., 2022).

Entre las principales modalidades destaca el ciberacoso, entendido como el uso de tecnologías digitales para vigilar, intimidar o amenazar a una persona, vulnerando su privacidad mediante programas capaces de acceder a mensajes, llamadas, contactos y otra información confidencial. En casos extremos, estas prácticas pueden derivar en situaciones de

violencia grave (Akrami et al., 2024). De igual forma, el software espía constituye una herramienta con aplicaciones legítimas de seguridad, pero también puede utilizarse de forma ilícita para monitorear ubicaciones, cuentas bancarias, comunicaciones, cámaras y micrófonos de las víctimas, convirtiéndose en un mecanismo invasivo que plantea importantes desafíos para la protección de la privacidad y el cumplimiento de la legislación vigente (Mustak et al., 2023).

El uso de software espía representa una de las principales herramientas empleadas para ejercer vigilancia y control sobre las víctimas, especialmente en contextos de violencia de pareja. Estas aplicaciones, comercializadas con fines legítimos como control parental o protección antirrobo, permiten el acceso remoto a información confidencial y, en muchos casos, evaden la detección de los sistemas antimalware, facilitando prácticas de intimidación, seguimiento y acoso. Asimismo, los ataques de denegación de servicio (DoS) y denegación de servicio distribuido (DDoS) provocan la interrupción de servicios y generan importantes pérdidas operativas y económicas (Akrami et al., 2024; Mustak et al., 2023).

La ciberdelincuencia comprende una amplia diversidad de modalidades que evolucionan constantemente, razón por la cual se han desarrollado taxonomías que clasifican los delitos dirigidos contra las personas, los sistemas y la información, a partir de evidencia científica y reportes gubernamentales (Phan et al., 2021; Monteith et al., 2021). Estas clasificaciones buscan facilitar la comprensión del fenómeno y adaptarse a la aparición de nuevas amenazas, incluyendo la ingeniería social, el acoso en línea, la piratería informática, los ataques de denegación de servicio y el ransomware, considerados entre los delitos más frecuentes en la actualidad (Tolba et al., 2021; van de Weijer & Moneva, 2022; Wissink et al., 2023). Desde la perspectiva criminológica, las organizaciones dedicadas al cibercrimen presentan estructuras jerarquizadas en las que participan miembros principales, facilitadores profesionales, facilitadores reclutados y mulas de dinero, quienes cumplen funciones específicas para ejecutar y ocultar las actividades ilícitas (Samreena, 2020). Además, estas redes pueden clasificarse según el grado de interacción entre delincuentes y víctimas, distinguiéndose organizaciones de baja y alta complejidad tecnológica (Zhong et al., 2020). Otros estudios identifican grupos que utilizan el ciberespacio para fortalecer delitos tradicionales, organizaciones que operan exclusivamente en línea, colectivos con motivaciones ideológicas o políticas y operaciones patrocinadas por los Estados, evidenciando la creciente sofisticación y diversidad del cibercrimen contemporáneo (Phillips et al., 2022; Drury et al., 2022).

Finalmente, estas organizaciones pueden adoptar configuraciones descentralizadas, como los grupos de tipo enjambre, o estructuras con centros de mando claramente definidos. Asimismo, existen modelos híbridos que combinan actividades delictivas en línea y fuera de línea, demostrando la capacidad de adaptación de las redes criminales frente a los avances tecnológicos y a las oportunidades que ofrece el entorno digital (Guerra et al., 2021). Las redes de ciberdelincuencia presentan distintos niveles de organización. Los grupos híbridos extendidos operan de forma descentralizada y están conformados por numerosos miembros y subgrupos, mientras que otros mantienen estructuras similares a las organizaciones criminales tradicionales o funcionan como agrupaciones temporales sin una jerarquía definida (Mustak et al., 2023). La

investigación también analiza el papel de los integrantes, sus relaciones, el liderazgo y el grado de utilización de la tecnología; sin embargo, aún existe escasa evidencia empírica sobre el funcionamiento interno de estas redes y, particularmente, sobre el rol desempeñado por los actores centrales (Qaiser, 2020).

Entre las modalidades más frecuentes destacan el fraude con tarjetas bancarias y las estafas telefónicas, delitos que aprovechan la digitalización de la información personal para obtener datos financieros y cometer robos de identidad (Kozik et al., 2022). La concentración de información en bases de datos gubernamentales y privadas incrementa la vulnerabilidad de los ciudadanos, ya que el acceso a identificadores personales o datos bancarios facilita la apropiación de identidades y la realización de fraudes con fines económicos (Monteith et al., 2021; Akhter et al., 2023). Para reducir estos riesgos se recomienda desconfiar de solicitudes de información confidencial recibidas por correo electrónico o redes sociales, monitorear periódicamente cuentas bancarias e informes crediticios y utilizar herramientas de seguridad que fortalezcan la protección de las credenciales de acceso (Brands y Van Doorn, 2022).

Las investigaciones también muestran que las redes de ciberdelincuencia han evolucionado hacia modelos descentralizados, conformados por células autónomas que se coordinan mediante plataformas digitales y foros clandestinos, como los mercados de *carding* en la *dark web*, donde intercambian herramientas de ataque, información robada y planifican operaciones sin una autoridad central claramente identificable (Nguyen y Luong, 2021). El ciberterrorismo constituye otra manifestación relevante del cibercrimen, al utilizar Internet y las redes sociales para difundir desinformación, generar miedo, alterar la opinión pública, afectar la estabilidad institucional y ocasionar daños a infraestructuras críticas, con consecuencias que pueden extenderse al ámbito político, social e incluso a la seguridad de las personas (Yongmei y Afzal, 2023).

La detección del ciberterrorismo constituye un desafío debido a que sus efectos suelen materializarse antes de ser identificados. En muchos casos, las víctimas desconocen que han sido objeto de campañas de desinformación o manipulación, por lo que su identificación requiere capacidades analíticas especializadas para reconocer contenidos falsos o descontextualizados que promueven el miedo, la violencia o la alteración del orden social (Stine y Barrett, 2022). De manera similar, el envío de mensajes engañosos o con contenido sexual constituye una modalidad delictiva que puede ocasionar graves consecuencias psicológicas, sociales y emocionales, especialmente cuando los delincuentes utilizan perfiles falsos o la suplantación de identidad para ganar la confianza de las víctimas (Ukam et al., 2024).

El ciberacoso comprende el uso de amenazas, intimidación, humillación o coerción mediante redes sociales y plataformas digitales, afectando principalmente a adolescentes y mujeres (Phillips et al., 2022). Entre sus manifestaciones más comunes se encuentran el abuso verbal en línea, la difusión no autorizada de contenido íntimo (*morphing*), la difamación y el chantaje mediante información personal, conductas que suelen repetirse y ocasionan importantes daños psicológicos y sociales (Brands y Van, 2022). La detección temprana requiere identificar patrones de hostigamiento, difusión de contenido falso o íntimo y el uso indebido de información personal con fines de intimidación

o extorsión (Choi et al., 2022). En el ámbito universitario, el ciberacoso y los delitos informáticos afectan la comunicación institucional, las relaciones interpersonales y el bienestar emocional de los estudiantes. Asimismo, favorecen la difusión de rumores, la suplantación de identidad y el robo de información personal y financiera, incrementando los riesgos de fraude y vulneración de la privacidad (Özaşçılar et al., 2024; Kozik et al., 2022). Además, los ciberdelincuentes utilizan herramientas de análisis de redes sociales, perfiles falsos y bots para recopilar información, seleccionar objetivos y ejecutar ataques de *phishing* y fraude con mayor precisión (Rawat, 2023).

Estos delitos también repercuten en los procesos educativos al interrumpir plataformas de aprendizaje virtual, comprometer información académica y limitar el acceso a recursos institucionales y actividades extracurriculares. Como consecuencia, pueden deteriorar la reputación de las instituciones de educación superior y disminuir la confianza de estudiantes y docentes en las tecnologías empleadas para la enseñanza y la gestión universitaria (Phan et al., 2021; Mabunda, 2024).

Materiales y Métodos

La investigación se diseñó de forma no experimental con un enfoque cuantitativo lo que permitió analizar las relaciones entre las variables sin intervenir en el entorno de los participantes. Se adoptó un diseño de investigación transversal y descriptivo-correlacional, que fue ideal para identificar y describir los efectos de los ciberdelitos en las actividades sociales y educativas de los estudiantes universitarios, así como para explorar las correlaciones entre diferentes tipos de ciberdelitos y sus impactos. El método cuantitativo se eligió porque facilitó la recopilación de datos numéricos que permitieron medir el nivel de impacto de los ciberdelitos de forma objetiva y precisa. Además, al ser un estudio transversal, se obtuvo información en un solo punto en el tiempo, lo que hizo posible observar las correlaciones sin requerir una observación prolongada. Este enfoque fue adecuado para proporcionar una "fotografía" del impacto actual de los ciberdelitos en la comunidad estudiantil de la Universidad de Guayaquil.

El tipo de investigación descriptivo-correlacional se centró, por un lado, en describir las características y la prevalencia de distintos tipos de ciberdelitos (como el robo de identidad, ciberacoso, ciberterrorismo, y contacto sospechoso) y, por otro, en examinar la relación entre estos delitos y las actividades académicas y sociales de los estudiantes. La investigación descriptiva permitió detallar la frecuencia y características de los ciberdelitos, mientras que el componente correlacional se utilizó para investigar cómo diferentes tipos de ciberdelitos afectan diversas dimensiones de la vida de los estudiantes.

Para recolectar los datos, se utilizó un cuestionario estructurado con escala tipo Likert (ver tabla 1), que se había utilizado y validado en estudios previos relacionados con la ciberseguridad y la victimización en línea (por ejemplo, el cuestionario desarrollado por Arpaci y Aslan, 2023, para medir la conciencia sobre ciberdelitos en redes sociales). Este instrumento se adaptó para que cubriera cuatro dimensiones clave de ciberdelitos identificadas como de particular relevancia para los estudiantes universitarios en Ecuador: el robo de identidad, el ciberacoso, el ciberterrorismo, y el contacto sospechoso. Cada dimensión incluyó una serie de afirmaciones a las que los

participantes respondieron en una escala de 5 puntos, que variaba de "totalmente en desacuerdo" a "totalmente de acuerdo". Las variables se calcularon de la siguiente forma (los códigos están en la tabla 1).

VI. Ciberdelitos= sum (CIRI1,CIRI2,CIRI3,CICA1,CICA2,CICA3,CICT1,CICT2,CICT3,CICS1,CICS2,CICS3)/12
VD1. Actividades Académicas= sum (AAIA1,AAIA2,AAIA3,AAAR1,AAAR2,AAAR3,AAPA1,AAPA2,AAPA3)/9
VD2. Actividades Sociales= sum(ASPS3,ASPS2,ASPS1,ASBE3,ASBE2)/5

Para asegurar la validez y confiabilidad del cuestionario, se realizó una validación previa mediante el Coeficiente Alfa de Cronbach, que resultó en un índice de confiabilidad de 0.984, indicando un alto nivel de consistencia interna del instrumento. La validación previa del cuestionario se llevó a cabo con un grupo piloto de 30 estudiantes antes de la recolección definitiva de los datos, lo que permitió ajustar las preguntas para maximizar la claridad y reducir posibles sesgos en las respuestas. La población de estudio estuvo constituida por 53 408 estudiantes matriculados en distintas facultades de la Universidad de Guayaquil, abarcando tanto niveles de pregrado como de posgrado. Para obtener una muestra representativa y homogénea, se utilizó un método de muestreo aleatorio estratificado. Se dividió a la población en grupos o estratos según sus facultades y carreras, lo que permitió asegurar que todas las áreas de estudio estuvieran representadas. Finalmente, se seleccionaron un total de 382 estudiantes (calculados al 95% de confianza y 5% de error de la población), cumpliendo con los criterios de ser estudiantes regulares con asistencia constante a clases, asegurando que los datos reflejaran adecuadamente la realidad del entorno académico. Se envió el enlace a las asociaciones de estudiantes y respondieron (26% de Ciencias Administrativas, 11% de la Facultad de Medicina, 17% de la Facultad de Leyes, 22% de la Facultad de Filosofía, 8% de la Facultad de Arquitectura, 8% de la Facultad de Economía y de la Facultad de Comunicación 5%, las demás facultadas aportaron con el 3% del total de encuestados).

El procedimiento de recolección de datos se realizó de manera presencial y virtual. Se aplicaron cuestionarios impresos en las facultades para aquellos estudiantes que asistían a clases presenciales, mientras que los estudiantes que participaban en cursos de educación a distancia completaron el cuestionario a través de una plataforma Google Formularios. Se garantizó la confidencialidad y el anonimato de los participantes en todas las etapas de la investigación para fomentar respuestas sinceras y sin presiones externas. Los datos recolectados se introdujeron en el programa estadístico SPSS 25 para su análisis. El análisis de los datos se llevó a cabo utilizando herramientas de estadística descriptiva y correlacional. Se calcularon frecuencias y porcentajes para describir la prevalencia de cada tipo de ciberdelito, así como medias y desviaciones estándar para analizar la gravedad percibida de los impactos en las actividades sociales y educativas. Posteriormente, se utilizaron análisis de correlación de Pearson para identificar las relaciones entre las variables y determinar cómo los diferentes tipos de ciberdelitos afectaban las dimensiones clave de la vida universitaria. Esta metodología proporcionó una base sólida para comprender la magnitud del problema de los ciberdelitos en el entorno universitario y permitió establecer correlaciones significativas que respaldan la importancia de abordar estos problemas a nivel institucional y educativo.

Tabla 1. *Variables y dimensiones.*

Código	Variable	Dimensión	Pregunta
CI-RI1	Ciberdelitos	Robo de Identidad	He sido víctima del robo de mi identidad en plataformas en línea.
CI-RI2			Alguien ha utilizado mis datos personales sin mi autorización en redes sociales.
CI-RI3			Estoy preocupado por la posibilidad de que mi información personal sea robada en línea.
CI-CA1		Ciberacoso	He recibido mensajes ofensivos o intimidantes en redes sociales.
CI-CA2			Me han acosado o molestado repetidamente a través de plataformas en línea.
CI-CA3			He sido víctima de ciberacoso durante el último año.
CI-CT1		Ciberterrorismo	He sido expuesto a mensajes que incitan al miedo o a la violencia en redes sociales.
CI-CT2			Me preocupa que el contenido en línea pueda estar diseñado para manipular o desinformar.
CI-CT3			Creo que las redes sociales se utilizan para difundir información que causa ansiedad o temor.
CI-CS1		Contacto Sospechoso	He recibido solicitudes sospechosas de contacto en plataformas en línea.
CI-CS2			Personas que no conozco me han enviado mensajes inapropiados en redes sociales.
CI-CS3			He tenido contacto no deseado con desconocidos a través de plataformas en línea.
AA-IA1	Actividades Académicas	Interrupción del Aprendizaje	He tenido problemas para concentrarme en mis estudios debido a incidentes en línea.
AA-IA2			El uso de dispositivos digitales ha afectado negativamente mi rendimiento académico.
AA-IA3			Las distracciones en redes sociales interfieren con mi capacidad para estudiar.
AA-AR1		Acceso a Recursos Académicos	Los ciberataques han afectado mi acceso a plataformas educativas en línea.
AA-AR2			He tenido dificultades para acceder a bibliotecas digitales o recursos académicos debido a problemas de seguridad en línea.
AA-AR3			Me preocupo por la seguridad de los recursos académicos a los que accedo en línea.
AA-PA1		Participación en Actividades	Incidentes de ciberdelitos me han desmotivado a participar en actividades académicas en línea.
AA-PA2			He dejado de asistir a clases virtuales debido al temor a la ciberseguridad.
AA-PA3			La preocupación por la seguridad en línea afecta mi participación en actividades académicas extracurriculares.
AS-IS1	Actividades Sociales	Interacción Social en Línea	El miedo a ser víctima de ciberdelitos ha reducido mi interacción social en línea.
AS-IS2			He evitado participar en eventos sociales en línea por temor a la privacidad.
AS-IS3			Me preocupa la seguridad cuando uso redes sociales para interactuar con amigos.
S-BE1		Bienestar Emocional	He experimentado ansiedad debido a interacciones negativas en redes sociales.
AS-BE2			Incidentes de ciberacoso han afectado mi bienestar emocional.
AS-BE3			Las interacciones en línea afectan mi estado de ánimo de manera negativa.
AS-PS1		Privacidad y Seguridad	Me preocupa que mi información personal pueda ser utilizada de manera inapropiada en línea.
AS-PS2			Me siento inseguro/a al compartir información personal en redes sociales.
AS-PS3			He tomado medidas para proteger mi privacidad debido a experiencias previas en línea.

Nota: Las preguntas de la encuesta son adaptadas de Arpaci y Aslan, (2023) y Yelaiev et al. (2024). Las respuestas a las preguntas fueron hechas en la escala de Likert en donde 1 es muy en desacuerdo y 5 muy de acuerdo.

Resultados y Discusión

La información presentada en la tabla 2 refleja la percepción y experiencias de los participantes en relación con los ciberdelitos y su impacto en actividades académicas y sociales. A continuación, se presenta un análisis detallado de los resultados empíricos de las encuestas: Robo de Identidad y Seguridad en Línea: Un 33% de los encuestados afirmó estar "muy en desacuerdo" con haber sido víctimas de robo de identidad, mientras que un 53.7% también indicó desacuerdo, sugiriendo que la mayoría de los participantes no han experimentado este tipo de incidentes. Sin embargo, un número considerable mostró preocupación sobre la posibilidad de que su información personal sea robada en línea, lo que indica un alto nivel de concienciación y percepción de riesgo, con un 24.1% en desacuerdo y un 53.4% en desacuerdo, pero un notable 9.9% "muy de acuerdo" con la preocupación. Ciberacoso: El 49.5% de los encuestados se mostró "muy en desacuerdo" con haber sido acosados repetidamente en plataformas en línea, y un 31.4% adicional también expresó desacuerdo, lo que sugiere que, aunque la mayoría no ha sido víctima, existe una minoría que sí lo ha experimentado, como lo evidencia el 12% que respondió "muy de acuerdo". Además, el 20.7% estuvo en desacuerdo con haber sido víctimas de ciberacoso durante el último año, pero una fracción significativa (12.3%) reconoció haber sufrido acoso en el mismo período.

Tabla 2. *Resultados de las encuestas.*

Preguntas de la investigación	Muy en desacuerdo	Desacuerdo	Indiferente	De acuerdo	Muy de acuerdo
He sido víctima del robo de mi identidad en plataformas en línea.	33,0%	53,7%	1,0%	8,1%	4,2%
Alguien ha utilizado mis datos personales sin mi autorización en redes sociales.	56,0%	30,4%	0,8%	5,5%	7,3%
Estoy preocupado por la posibilidad de que mi información personal sea robada en línea.	24,1%	53,4%	1,6%	11,0%	9,9%
He recibido mensajes ofensivos o intimidantes en redes sociales.	24,1%	55,8%	1,3%	6,8%	12,0%
Me han acosado o molestado repetidamente a través de plataformas en línea.	49,5%	31,4%	1,0%	6,0%	12,0%
He sido víctima de ciberacoso durante el último año.	20,7%	58,1%	2,4%	6,5%	12,3%
He sido expuesto a mensajes que incitan al miedo o a la violencia en redes sociales.	20,7%	56,3%	0,8%	9,9%	12,3%
Me preocupa que el contenido en línea pueda estar diseñado para manipular o desinformar.	31,7%	51,8%	1,3%	2,9%	12,3%
Creo que las redes sociales se utilizan para difundir información que causa ansiedad o temor.	27,0%	56,3%	1,3%	7,9%	7,6%
He recibido solicitudes sospechosas de contacto en plataformas en línea.	32,5%	42,4%	1,3%	14,9%	8,9%
Personas que no conozco me han enviado mensajes inapropiados en redes sociales.	24,1%	53,9%	1,0%	11,3%	9,7%
He tenido contacto no deseado con desconocidos a través de plataformas en línea.	24,3%	52,9%	1,8%	10,5%	10,5%
He tenido problemas para concentrarme en mis estudios debido a incidentes en línea.	27,0%	54,5%	1,0%	4,5%	13,1%
El uso de dispositivos digitales ha afectado negativamente mi rendimiento académico.	17,8%	62,6%	1,8%	7,9%	9,9%
Las distracciones en redes sociales interfieren con mi capacidad para estudiar.	21,2%	57,1%	1,8%	10,2%	9,7%
Los ciberataques han afectado mi acceso a plataformas educativas en línea.	12,0%	65,2%	1,8%	6,0%	14,9%

Fuente: Elaboración propia.

Tabla 3. *Resultados de las encuestas (continuación)*

Preguntas de la investigación	Muy en desacuerdo	Desacuerdo	Indiferente	De acuerdo	Muy de acuerdo
He tenido dificultades para acceder a bibliotecas digitales o recursos académicos debido a problemas de seguridad en línea.	15,2%	63,6%	1,6%	2,9%	16,8%
Me preocupo por la seguridad de los recursos académicos a los que accedo en línea.	16,5%	61,0%	1,6%	5,8%	15,2%
Incidentes de ciberdelitos me han desmotivado a participar en actividades académicas en línea.	20,4%	58,4%	1,8%	10,7%	8,6%
He dejado de asistir a clases virtuales debido al temor a la ciberseguridad.	29,6%	49,0%	1,8%	2,9%	16,8%
La preocupación por la seguridad en línea afecta mi participación en actividades académicas extracurriculares.	27,2%	53,9%	1,8%	3,4%	13,6%
El miedo a ser víctima de ciberdelitos ha reducido mi interacción social en línea.	60,2%	21,2%	0,8%	10,7%	7,1%
He evitado participar en eventos sociales en línea por temor a la privacidad.	28,5%	46,1%	2,4%	14,9%	8,1%
Me preocupa la seguridad cuando uso redes sociales para interactuar con amigos.	11,3%	67,3%	1,3%	11,0%	9,2%
He experimentado ansiedad debido a interacciones negativas en redes sociales.	28,3%	46,1%	1,0%	8,9%	15,7%
Incidentes de ciberacoso han afectado mi bienestar emocional.	28,3%	46,1%	1,0%	8,9%	15,7%
Las interacciones en línea afectan mi estado de ánimo de manera negativa.	28,3%	46,1%	1,0%	8,9%	15,7%
Me preocupa que mi información personal pueda ser utilizada de manera inapropiada en línea.	28,3%	46,1%	1,0%	8,9%	15,7%
Me siento inseguro/a al compartir información personal en redes sociales.	28,3%	46,1%	1,0%	8,9%	15,7%
He tomado medidas para proteger mi privacidad debido a experiencias previas en línea.	19,6%	47,9%	1,6%	17,3%	13,6%

Fuente: Elaboración propia.

Interacciones Inseguras y Contenido Manipulador: La preocupación sobre las interacciones en línea se ve reflejada en el hecho de que el 32.5% de los participantes han recibido solicitudes sospechosas de contacto, lo que destaca un problema latente de seguridad. Un 31.7% señaló preocupación por el contenido manipulado para desinformar o incitar temor, indicando la creciente necesidad de abordar estos riesgos de manera preventiva.

Distracciones y Seguridad en Plataformas Educativas: Los datos sugieren que las distracciones derivadas del uso de redes sociales interfieren en la capacidad de estudio, con el 21.2% "muy en desacuerdo" y un notable 57.1% en desacuerdo con dicha afirmación. Sin embargo, los problemas de ciberseguridad que afectan el acceso a plataformas educativas preocupan al 15.2% de los participantes, quienes están "muy de acuerdo" en que han tenido dificultades para acceder a recursos académicos debido a problemas de seguridad en línea. Esto indica que los ciberataques no solo impactan a nivel personal sino también en el entorno educativo, dificultando el acceso a la educación digital.

Efectos en el Rendimiento Académico: Un 17.8% no considera que los dispositivos digitales hayan afectado negativamente su rendimiento académico, pero la alta cifra del 62.6% en desacuerdo señala que existe una percepción general de que las tecnologías digitales pueden tener efectos negativos si no se gestionan adecuadamente. Además, la preocupación por la ciberseguridad ha hecho que algunos estudiantes, el 29.6%, consideren dejar de asistir a clases virtuales, lo que subraya el impacto directo de los riesgos en línea en la educación. Ansiedad y Bienestar Emocional: La información destaca que las interacciones en línea generan ansiedad, como indicó el 28.3% de los encuestados. Los datos también señalan que el ciberacoso afecta el bienestar emocional de los estudiantes, con el 28.3% en desacuerdo sobre no verse afectados, pero con un 15.7% que confirma el impacto emocional negativo derivado de estas experiencias. Esto muestra que las interacciones en plataformas digitales tienen un efecto considerable en la salud mental y emocional.

Protección de la Privacidad: El 28.3% mostró preocupación sobre la posible utilización inapropiada de su información personal en línea, y un 19.6% ha tomado medidas para proteger su privacidad debido a experiencias previas, lo que evidencia un grado considerable de prevención proactiva entre los usuarios. Las preocupaciones sobre seguridad en redes sociales fueron destacadas por el 11.3% que expresó incertidumbre sobre su uso para interactuar con amigos, y un 67.3% adicional que reflejó inseguridad.

Los datos indican que, aunque una mayoría significativa no ha sido víctima directa de incidentes graves como robo de identidad o ciberacoso, existe una preocupación latente sobre la posibilidad de que ocurran. Además, el impacto de estos ciberdelitos se manifiesta en la vida académica y social de los estudiantes, afectando el acceso a la educación, el rendimiento académico y el bienestar emocional. Esto sugiere que las instituciones deben considerar medidas preventivas y educativas más robustas para abordar estos problemas de manera integral.

La tabla 3 de correlaciones presentada ofrece una visión clara de la relación entre las tres variables principales de estudio: Ciberdelitos**,** Actividades Académicas **y** Actividades Sociales**.** Para analizar estos resultados, se han utilizado los coeficientes de correlación de Spearman, que indican el grado y la dirección de la relación entre las variables, así como su significancia estadística. Correlación entre Ciberdelitos y Actividades Académicas: El coeficiente de correlación entre Ciberdelitos y Actividades Académicas es 0.851, lo cual indica una correlación positiva fuerte. Esto significa que a medida que aumentan los incidentes relacionados con ciberdelitos, existe una tendencia a que las actividades académicas

se vean más afectadas. La significancia estadística (Sig. bilateral) de 0.000 confirma que esta correlación es estadísticamente significativa al nivel del 0.01.

Tabla 4. *Correlación de variables.*

Rho de Spearman		Ciberdelitos	Actividades Académicas	Actividades Sociales
Ciberdelitos	Coeficiente de correlación	1,000	,851**	,839**
	Sig. (bilateral)		0,000	0,000
	N	382	382	382
Actividades Académicas	Coeficiente de correlación	,851**	1,000	,914**
	Sig. (bilateral)	0,000		0,000
	N	382	382	382
Actividades Sociales	Coeficiente de correlación	,839**	,914**	1,000
	Sig. (bilateral)	0,000	0,000	
	N	382	382	382
Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).				

Fuente: Elaboración propia.

Este resultado sugiere que hay una relación considerable entre la exposición a ciberdelitos y el rendimiento o la participación en actividades académicas, indicando posibles efectos adversos sobre la educación de los estudiantes. Correlación entre Ciberdelitos y Actividades Sociales: La relación entre Ciberdelitos y Actividades Sociales muestra un coeficiente de 0.839, que también señala una correlación positiva fuerte. Al igual que en el caso anterior, el valor de significancia es 0.000, lo que indica que la correlación es estadísticamente significativa.

Este hallazgo sugiere que las experiencias o preocupaciones relacionadas con ciberdelitos también afectan las actividades sociales de los estudiantes. Las implicaciones pueden incluir una disminución en la participación en interacciones sociales en línea o en persona, debido a temores sobre la privacidad y la seguridad digital. Correlación entre Actividades Académicas y Actividades Sociales: La correlación entre Actividades Académicas y Actividades Sociales es la más alta, con un coeficiente de 0.914. Esta fuerte correlación positiva indica que las experiencias en el ámbito académico y social están estrechamente relacionadas; cuando una se ve afectada, es probable que la otra también lo esté. Nuevamente, el valor de significancia es 0.000, confirmando la relevancia estadística de la correlación. Esto podría interpretarse como que los problemas en la vida académica, posiblemente exacerbados por ciberdelitos, también repercuten en la vida social de los estudiantes, y viceversa.

Los resultados de las correlaciones sugieren que los ciberdelitos tienen un impacto significativo tanto en las actividades académicas como en las sociales de los estudiantes. Las altas correlaciones positivas entre estas variables destacan la interconexión de estos aspectos de la vida estudiantil. La presencia de ciberdelitos parece ser un factor que influye negativamente, afectando no solo el rendimiento académico sino también la vida social de los individuos. Los valores de significancia (todos a 0.000) aseguran que las correlaciones observadas no son producto del azar, reforzando la importancia de implementar medidas de seguridad digital para proteger tanto la educación como las interacciones sociales de los estudiantes universitarios.

Conclusiones

La sección de Conclusiones en un artículo El presente estudio ha explorado la intersección

entre los ciberdelitos y su impacto en la vida social y académica de los estudiantes universitarios, enfocándose en la Universidad de Guayaquil. Los resultados obtenidos reflejan una realidad preocupante que afecta a la comunidad universitaria y subrayan la necesidad urgente de implementar estrategias legales, políticas y educativas para mitigar estos efectos. Los hallazgos de la investigación coinciden con estudios previos y aportan nuevos conocimientos que pueden servir de guía para futuras intervenciones en el ámbito académico y social.

A lo largo del estudio se ha evidenciado que los ciberdelitos tienen un impacto significativo tanto en las actividades académicas como en las sociales de los estudiantes. Los datos obtenidos a través de la encuesta reflejan que los estudiantes han sido víctimas de diversas formas de ciberdelitos, desde el robo de identidad y ciberacoso hasta el contacto no deseado y el ciberterrorismo. El análisis de correlaciones muestra una relación positiva y significativa entre la exposición a ciberdelitos y los efectos negativos en la vida académica y social de los estudiantes.

Los resultados son consistentes con los estudios de Griffith et al. (2023) y Guedes et al. (2023), quienes identificaron cómo la victimización y el miedo al robo de identidad afectan las actividades sociales y educativas de los jóvenes. Además, coinciden con las observaciones de Lucero (2023), que se centraron en la violación de derechos fundamentales como la privacidad e integridad a causa de los ciberdelitos. Esto destaca la necesidad de desarrollar políticas educativas que promuevan la concienciación y educación sobre ciberseguridad entre los estudiantes, así como la creación de espacios seguros para la denuncia de este tipo de agresiones. La investigación ha permitido confirmar que los ciberdelitos afectan de manera negativa la normalidad social y educativa de los estudiantes. Esto se refleja en el alto porcentaje de encuestados que reportaron preocupación por la posibilidad de que su información personal sea robada y por el impacto que las interacciones en línea tienen en su bienestar emocional. Los estudios de AllahRakha (2024) y Sharma et al. (2023) argumentan que la globalización digital ha permitido que los ciberdelitos trasciendan fronteras, planteando desafíos adicionales para la seguridad jurídica, algo que se corrobora con los resultados obtenidos en el presente estudio, en el que los estudiantes expresan ansiedad y desconfianza hacia las plataformas digitales utilizadas en su día a día académico.

Asimismo, la correlación significativa encontrada entre los ciberdelitos y las actividades académicas resalta cómo el miedo a ser víctimas de delitos en línea puede influir en la disminución del rendimiento académico y la participación en actividades extracurriculares. Esta relación se alinea con las investigaciones de Mabunda (2024), que aplicaron la teoría de las actividades rutinarias para analizar cómo la exposición a ciber amenazas afecta el desempeño académico y las dinámicas sociales. Una de las conclusiones más claras que se derivan del estudio es la urgente necesidad de que las autoridades universitarias implementen estrategias legales y políticas para abordar los desafíos que presentan los ciberdelitos. Como señalan Cuenca y Núñez (2024), la falta de seguridad jurídica puede llevar a la impunidad de los perpetradores y afectar la confianza de las víctimas en las instituciones. Esto sugiere que las universidades deben colaborar estrechamente con entidades gubernamentales y tecnológicas para desarrollar políticas que no solo protejan a los estudiantes, sino que también promuevan una cultura de ciberseguridad. Por

otro lado, los estudios de Yongmei y Afzal (2023) demuestran que la implementación de leyes preventivas y marcos legales sólidos en otros países ha sido efectiva para reducir la incidencia de ciberdelitos. Esto debe tomarse como un ejemplo para Ecuador, donde las medidas legales aún son insuficientes para lidiar con las formas complejas y transnacionales que han adoptado estos delitos. La creación de mecanismos de denuncia más accesibles y el desarrollo de campañas educativas para sensibilizar a los estudiantes sobre los riesgos y precauciones en el ciberespacio son esenciales.

Para contrarrestar los efectos negativos de los ciberdelitos en la comunidad estudiantil universitaria, se sugieren las siguientes medidas basadas en los resultados obtenidos y en la revisión de la literatura: Implementar talleres y seminarios regulares que enseñen a los estudiantes cómo proteger su información personal en línea y reconocer comportamientos sospechosos. Estos programas deben estar diseñados para diferentes niveles de conocimiento y adaptarse a la realidad tecnológica que enfrentan los estudiantes hoy en día. Como se evidenció en el trabajo de Rawat (2023), la educación sobre ciberseguridad es clave para evitar que los estudiantes caigan en tácticas de manipulación y fraude en línea.

Las universidades deben establecer políticas claras que definan cómo se manejarán los casos de ciberacoso y robo de identidad, asegurando que las víctimas reciban apoyo psicológico y asesoramiento legal. Según Drury et al. (2022), el apoyo institucional es vital para que las víctimas puedan recuperarse emocionalmente y tomar medidas para evitar futuras agresiones. Las instituciones deben garantizar que las plataformas utilizadas para educación en línea sean seguras y estén protegidas contra posibles ciberataques. Esto incluye la actualización constante de sistemas de seguridad y la realización de auditorías regulares. Los resultados de la encuesta mostraron que un porcentaje significativo de estudiantes han experimentado dificultades para acceder a plataformas educativas debido a problemas de seguridad, lo que afecta directamente su rendimiento académico.

Establecer un equipo especializado dentro de la universidad que pueda monitorear, responder y mitigar incidentes de ciberdelitos en tiempo real. Este equipo también podría proporcionar asesoría personalizada a estudiantes que necesiten ayuda para navegar situaciones de riesgo. El estudio de Pawlak et al. (2020) sugiere que la preparación y respuesta rápida son clave para limitar el impacto de los ciberataques y reducir el daño potencial a las víctimas. El estudio actual corrobora muchos de los hallazgos presentes en la literatura, pero también aporta nuevas perspectivas sobre la realidad en Ecuador.

Mientras que investigaciones en otros países, como las de Phillips et al. (2022) y Stine y Barrett (2022), se han centrado en la proliferación de ciberdelitos en contextos de infraestructura crítica, el presente trabajo se adentra en las consecuencias personales que enfrentan los estudiantes universitarios al ser expuestos a estas amenazas. Asimismo, se identificaron patrones de comportamiento que se alinean con los de otros estudios. Por ejemplo, los ciberdelitos como el ciberacoso y el robo de identidad se presentan de manera similar en la universidad de Guayaquil y en otros contextos globales, tal como se mencionó en los estudios de Nguyen y Luong (2021) y Kozik et al. (2022). Sin embargo, en Ecuador, se observa una desconfianza particular hacia las plataformas digitales educativas, lo que puede

estar relacionado con la falta de recursos tecnológicos y el desconocimiento sobre ciberseguridad.

A partir de los resultados, se recomienda que futuras investigaciones se enfoquen en estudios longitudinales que permitan analizar la evolución de los efectos de los ciberdelitos en la vida académica y social de los estudiantes a lo largo del tiempo. Esto ayudará a entender mejor las estrategias de adaptación que desarrollan las víctimas y a identificar patrones que no pueden ser observados en estudios transversales. Además, sería valioso investigar diferencias demográficas y cómo factores como el género, la edad y el nivel socioeconómico influyen en la exposición y percepción de riesgos relacionados con ciberdelitos. En conclusión, el estudio destaca la urgencia de abordar la ciberdelincuencia en el entorno universitario de manera integral, implementando estrategias educativas, legales y tecnológicas que protejan a los estudiantes y fomenten un ambiente seguro para el desarrollo académico y social. Las universidades deben jugar un papel activo en la prevención y gestión de riesgos cibernéticos, y su compromiso en esta área será clave para fortalecer la confianza de los estudiantes en el uso seguro de tecnologías digitales.

Referencias Bibliográficas

Akhter, A., Acharjee, U., Talukder, M., Islam, M., & Uddin, M. (2023). A robust hybrid machine learning model for Bengali cyber bullying detection in social media. *Natural Language Processing Journal, 4*, 100027. https://doi.org/10.1016/j.nlp.2023.100027

Akrami, K., Akrami, M., Akrami, F., Ahrari, M., Hakimi, M., & Fazil, A. (2024). Investigating the adverse effects of social media and cybercrime in higher education: A case study of an online university. *Studies in Media, Journalism and Communications, 2*(1), 22–33.

AllahRakha, N. (2024). Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy, 2*(2). https://irshadjournals.com/index.php/ijlp/article/view/156

Álvarez, A., Del Aguila, S., Rosen, M., García, V., Maycotte, S., & Martínez, G. (2021). Expectations and interests of university students in COVID-19 times about Sustainable Development Goals: Evidence from Colombia, Ecuador, Mexico, and Peru. *Sustainability, 13*(6), Article 3306. https://doi.org/10.3390/su13063306

Arpaci, I., & Aslan, O. (2023). Development of a scale to measure cybercrime-awareness on social media. *Journal of Computer Information Systems, 63*(3), 695–705. https://doi.org/10.1080/08874417.2022.2101160

Brands, J., & Van Doorn, J. (2022). La medición, intensidad y determinantes del miedo al cibercrimen: Una revisión sistemática. *Computers in Human Behavior, 127*, 107082. https://doi.org/10.1016/j.chb.2021.107082

Chandra, A., & Snowe, M. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems, 38*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Chang, W. (2020). Cyberstalking and law enforcement. *Procedia Computer Science, 176*, 1188–1194. https://doi.org/10.1016/j.procs.2020.09.115

Choi, J., Kruis, N., & Lee, J. (2022). Empathy, self-control, and online harassment: A partial test of Agnew's social concern theory. *Computers in Human Behavior, 136*, 107402. https://doi.org/10.1016/j.chb.2022.107402

Cook, S., Giommoni, L., Trajtenberg, N., Levi, M., & Williams, M. (2023). Fear of economic cybercrime across Europe: A multilevel application of Routine Activity Theory. *The British Journal of Criminology, 63*(2), 384–406.

Cuenca, A., & Núñez, J. (2024). Análisis documental: Impacto de la seguridad jurídica ante los delitos informáticos. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5*(4), 2541–2551.

Del Pezo, E. (2023). *La eficacia o ineficacia de la evidencia digital como elemento probatorio en el juzgamiento de los delitos informáticos* [Tesis de licenciatura, Universidad Estatal Península de Santa Elena]. https://repositorio.upse.edu.ec/handle/46000/10357

Drury, B., Drury, S., Rahman, M., & Ullah, I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media, 30*, 100211. https://doi.org/10.1016/j.osnem.2022.100211

Ene, W., & Imo, A. (2024). Cybercrime and its implications for human capital development: A study of Otuoke Community, FUO students. *Fuoye Journal of Criminology and Security Studies, 3*(2). https://fjcss.fuoye.edu.ng/index.php/fjcss/article/view/97

Griffith, C., Tetzlaff-Bemiller, M., & Hunter, L. (2023). Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports, 9*, 100042.

Guedes, I., Martins, M., & Cardoso, C. (2023). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal, 36*(3), 472–497. https://doi.org/10.1057/s41284-022-00350-5

Guerra, C., Pinto-Cortez, C., Toro, E., Efthymiadou, E., & Quayle, E. (2021). Online sexual harassment and depression in Chilean adolescents: Variations based on gender and age of the offenders. *Child Abuse & Neglect, 120*, 105219. https://doi.org/10.1016/j.chiabu.2021.105219

Jobi Babu, D., Thomas, B., & Kübra, S. (2024). Enhancing women's knowledge on cyber sexual offenses through AI-based education and awareness. *Library Progress International, 44*(3), 4446–4457.

Keenlyside, A., Hernández, S., & Font, I. (2021). El delito de «sexting» o difusión de imágenes obtenidas con anuencia y sin consentimiento. *Revista Aranzadi Doctrinal, 1*.

Kozik, R., Kula, S., Choraś, M., & Woźniak, M. (2022). Technical solution to counter potential crime: Text analysis to detect fake news and disinformation. *Journal of Computational Science, 60*, 101576. https://doi.org/10.1016/j.jocs.2022.101576

Lucero, J. (2023). *Delitos informáticos y la violación de los derechos constitucionales de integridad e intimidad* [Tesis doctoral, Pontificia Universidad Católica del Ecuador]. https://repositorio.puce.edu.ec/bitstreams/0fa955c0-eac5-463d-9d3c-61bb897ba99e/download

Mabunda, S. (2024). Applying the Routine Activities Theory to cybercrime: A 'cyber' capable guardian. *Journal of Anti-Corruption Law, 8*, 60–84.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports, 23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research, 154*, 113368. https://doi.org/10.1016/j.jbusres.2022.113368

Nguyen, T., & Luong, H. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice, 44*(4), 419–440. https://doi.org/10.1080/0735648X.2020.1818605

Özaşçılar, M., Çalıcı, C., & Vakhitova, Z. (2024). Examining cybercrime victimisation among Turkish women using Routine Activity Theory. *Crime Prevention and*

Community Safety, 26(1), 112–128. https://doi.org/10.1057/s41300-024-00201-y

Pawlak, P., Abdel-Sadek, A., Dominioni, S., & Youmna, A. (2020). Great expectations: Defining a trans-Mediterranean cybersecurity agenda. *European View, 22*, 85.

Phan, A., Seigfried-Spellar, K., & Choo, K. (2021). Threaten me softly: A review of potential dating app risks. *Computers in Human Behavior Reports, 3*, 100055. https://doi.org/10.1016/j.chbr.2021.100055

Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Qaiser, S. (2020). *Cyber crime: Rise, evolution and prevention*. https://doi.org/10.13140/RG.2.2.18533.01762

Quirumbay, D., Castillo, C., & Coronel, I. (2022). *Una revisión del aprendizaje profundo aplicado a la ciberseguridad*. Universidad Estatal Península de Santa Elena. https://repositorio.upse.edu.ec/handle/46000/8231

Rawat, R. (2023). Logical concept mapping and social media analytics relating to cyber criminal activities for ontology creation. *International Journal of Information Technology, 15*(2), 893–903. https://doi.org/10.1007/s41870-022-00934-9

Sharma, V., Manocha, T., Garg, S., Sharma, S., Garg, A., & Sharma, R. (2023). Growth of cyber-crimes in Society 4.0. En *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1–6). IEEE. https://ieeexplore.ieee.org/abstract/document/10118185/

Singh, A., Chawla, P., Krishnamurthi, R., & Kumar, A. (2022). Delitos cibernéticos y enfoques de defensa en redes vehiculares. En R. Krishnamurthi, A. Kumar, & S. Gill (Eds.), *Autonomous and Connected Heavy Vehicle Technology* (pp. 37–63). Academic Press. https://doi.org/10.1016/B978-0-323-90592-3.00002-1

Stine, K., & Barrett, M. (2022). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Spanish translation)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018es

Tolba, M., Ouadfel, S., & Meshoul, S. (2021). Hybrid ensemble approaches to online harassment detection in highly imbalanced data. *Expert Systems with Applications, 175*, 114751. https://doi.org/10.1016/j.eswa.2021.114751

Ukam, P., Onuh, P., Nnaji, D., Egbo, E., & Ugwu, C. (2024). How engagement in internet fraud impacts academic activities of undergraduate students in Nigeria: A socio-legal study. *Cogent Social Sciences, 10*(1), 2280285. https://doi.org/10.1080/23311886.2023.2280285

Van de Weijer, S., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports, 8*, 100249. https://doi.org/10.1016/j.chbr.2022.100249

Wall, D. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons. https://books.google.es/books?hl=es&lr=&id=DIMCEQAAQBAJ

Wissink, I., Standaert, J., Stams, G., Asscher, J., & Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. *Aggression and Violent Behavior, 70*, 101836. https://doi.org/10.1016/j.avb.2023.101836

Yelaiev, Y., Fedchak, I., Senyk, V., Tymchyshyn, D., & Nazarenko, P. (2024). Effectiveness of forensic computer modeling for predicting wartime crimes. *Pakistan Journal of Criminology, 16*(2). https://dspace.lvduvs.edu.ua/bitstream/1234

567890/7267/1/40-Effectiveness-of-Forensic-Computer-Modelling.pdf

Yongmei, C., & Afzal, J. (2023). Impact of enactment of the Prevention of Electronic Crimes Act, 2016 as legal support in Pakistan. *Academy of Education and Social Sciences Review, 3*(2), 203–212.

Zhong, L., Kebbell, M., & Webster, J. (2020). An exploratory study of technology-facilitated sexual violence in online romantic interactions: Can the Internet's toxic disinhibition exacerbate sexual aggression? *Computers in Human Behavior, 108*, 106314. https://doi.org/10.1016/j.chb.2020.106314

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT) Alberto Emmanuel Cárdenas Bolaños: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio. Hugo Alberto Cárdenas Echeverría: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.
Declaración de conflicto de intereses Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.
Declaración del editor El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.
Declaración de los revisores Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.
Declaración sobre el uso de inteligencia artificial Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.
Disponibilidad de datos Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.