Artículo Científico

BLEZ TECNOLÓGICO ONLINE

CEC Revista Científica Enfoques del Conocimiento

ISSN: 3151-8486

Ciberdelitos y desafíos legales en la protección de datos personales y privacidad digital

Cybercrime and legal challenges in the protection of personal data and digital privacy

Castro-Morales, Samuel [1]
https://orcid.org/0000-0003-1753-2516
samuel.morales-externo@unir.net
España, La Rioja, Universidad Internacional de la Rioja.

Samaniego-Quiguiri, Delia Paulina [2]
https://orcid.org/0000-0002-2051-3431
samaniegod@fiscalia.gob.ec
Ecuador, Bolivar, Fiscalía General del Estado.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/revistacec/v2/n1/27

Resumen: La acelerada digitalización de servicios públicos, financieros, educativos, comerciales y sociales en Latinoamérica ha incrementado la exposición de datos personales frente a fraudes, accesos indebidos, filtraciones, ransomware, phishing y suplantación de identidad, generando riesgos económicos, jurídicos e institucionales. El estudio tuvo como objetivo analizar la relación entre los ciberdelitos y los desafíos legales vinculados con la protección de datos personales y la privacidad digital en la región. Se desarrolló una investigación documental, cualitativa, exploratoria e interpretativa, basada en literatura científica, doctrina jurídica, informes técnicos, marcos normativos y documentos institucionales publicados entre 2014 y 2025. Los resultados evidencian que los ciberdelitos predominantes comprometen principalmente credenciales, documentos de identidad, datos financieros, registros administrativos, información de salud y datos de menores, mientras persisten brechas normativas, limitada notificación de incidentes, escasa madurez institucional y debilidades técnicas de respuesta. La discusión sostiene que la privacidad digital no puede protegerse mediante normas aisladas ni soluciones tecnológicas fragmentadas, sino mediante gobernanza integral de la ciberseguridad. Se concluye que Latinoamérica requiere fortalecer marcos legales, capacidades institucionales, cooperación regional y cultura organizacional para prevenir, contener, sancionar y reparar los daños derivados de la criminalidad informática.

Palabras clave: ciberdelitos; protección de datos; privacidad digital; ciberseguridad; Latinoamérica.

Check for updates

Received: 18/Nov/2024
Accepted: 20/Dic/2024
Published: 16/Ene/2025

Cita: Castro-Morales, S., & Samaniego-Quiguiri, D. P. (2025). Ciberdelitos y desafíos legales en la protección de datos personales y privacidad digital. *Revista Científica Enfoques Del Conocimiento*, *2*(1), 1-18. https://doi.org/10.55813/gaea/revistacec/v2/n1/27

Revista Científica Enfoques del Conocimiento (RCEC)
https://www.blez.edu.ec
https://revistacec.blez.edu.ec
revistacec@blez.edu.ec

Abstract:

The accelerated digitalization of public, financial, educational, commercial, and social services in Latin America has increased the exposure of personal data to fraud, unauthorized access, data breaches, ransomware, phishing, and identity theft, generating economic, legal, and institutional risks. This study aimed to analyze the relationship between cybercrime and the legal challenges associated with personal data protection and digital privacy in the region. A documentary, qualitative, exploratory, and interpretative research design was applied, based on scientific literature, legal doctrine, technical reports, regulatory frameworks, and institutional documents published between 2014 and 2025. The results show that the most prevalent cybercrimes mainly compromise credentials, identity documents, financial data, administrative records, health information, and children's data, while regulatory gaps, limited incident notification mechanisms, low institutional maturity, and technical weaknesses in response capacities persist. The discussion argues that digital privacy cannot be protected through isolated legal rules or fragmented technological solutions, but requires comprehensive cybersecurity governance. It is concluded that Latin America needs to strengthen legal frameworks, institutional capacities, regional cooperation, and organizational culture to prevent, contain, sanction, and repair the harms caused by cybercrime.

Keywords: cybercrime; data protection; digital privacy; cybersecurity; Latin America.

1. Introducción

La expansión de servicios digitales, comercio electrónico, banca móvil, gobierno digital y plataformas sociales ha convertido los datos personales en un recurso estratégico para la vida cotidiana en Latinoamérica, pero también en un objetivo central de economías ilícitas basadas en fraude, extorsión, suplantación de identidad, acceso indebido y filtración de información sensible. En este escenario, los ciberdelitos no pueden entenderse solo como fallas técnicas, sino como fenómenos sociojurídicos que tensionan la privacidad digital, la seguridad de la información y la capacidad estatal para prevenir, investigar y sancionar conductas transfronterizas. La magnitud del problema ya es verificable: en 2023, el 30% de las organizaciones latinoamericanas reportó al menos un incidente de seguridad, y los sectores más expuestos fueron gobierno, informática/tecnología y banca/finanzas, precisamente aquellos que concentran datos masivos de ciudadanos y usuarios (ESET, 2024; Solove, 2006).

La gravedad del fenómeno se amplifica porque las afectaciones no se agotan en la pérdida de archivos o credenciales, sino que alcanzan costos económicos, reputacionales e institucionales que deterioran la confianza pública en los servicios digitales. En 2024, el costo promedio de una filtración de datos en Latinoamérica llegó

a US$2,76 millones, 12% más que el año anterior; además, las industrias con mayor impacto fueron el sector industrial con US$3,54 millones, el financiero con US$3,22 millones y el de servicios con US$2,94 millones, mientras que el phishing representó el 16% de los incidentes y costó en promedio US$2,91 millones por filtración (IBM, 2024; Acquisti et al., 2015). La ausencia de respuestas coordinadas puede normalizar la vigilancia abusiva, el robo de identidad, la extorsión digital y la interrupción de servicios esenciales, con efectos diferenciados sobre personas, empresas y administraciones públicas (Nissenbaum, 2004).

El marco normativo regional muestra avances relevantes, aunque desiguales, porque la protección de datos personales ha progresado con mayor velocidad que la gobernanza integral de la ciberseguridad. Un estudio comparado de 33 países de América Latina y el Caribe identificó que 22 cuentan con legislación vigente en protección de datos personales y que todos esos 22 tienen una autoridad de control; sin embargo, 11 países todavía carecen de una ley en la materia, lo que fragmenta la tutela efectiva de derechos y dificulta la cooperación transfronteriza (Comisión Económica para América Latina y el Caribe {CEPAL}, 2024; Organización de los Estados Americanos {OEA}, 2021). La brecha es más visible cuando se observa que 21 de los 22 países con normativa prevén obligaciones de seguridad sobre los datos, pero solo 11 incorporan mecanismos de gestión de incidentes, y 18 de los 33 países no cuentan con lineamientos nacionales de notificación de incidentes (CEPAL, 2024).

La literatura especializada ha explicado que el cibercrimen transforma el delito tradicional al permitir acciones automatizadas, masivas y de bajo costo marginal, mientras que la teoría de la privacidad ha mostrado que el daño no se limita a la divulgación, sino que incluye recolección indebida, agregación, inseguridad, uso secundario e intrusión contextual (Wall, 2007; Solove, 2006; Nissenbaum, 2004). Pese a ello, los estudios sobre Latinoamérica suelen concentrarse en descripciones normativas por país o en diagnósticos técnicos de amenazas, dejando menos exploradas las relaciones entre capacidad institucional, obligación de notificar incidentes, madurez de CERT/CSIRT, costos de filtración, cumplimiento empresarial y derechos de los titulares. La inconsistencia importa porque la región puede exhibir leyes formales y, al mismo tiempo, debilidades operativas: solo 7 países cuentan con CERT/CSIRT gubernamental con mandato nacional, 12 no poseen CERT/CSIRT, y apenas Chile cuenta con una ley específica de ciberseguridad (CEPAL, 2024; Hoofnagle et al., 2019).

La pertinencia de estudiar conjuntamente ciberdelitos y desafíos legales radica en que la privacidad digital se vuelve ineficaz cuando la legislación no se articula con capacidades reales de prevención, detección, respuesta, sanción y reparación. En términos sociales, el análisis permite proteger a usuarios frente a fraudes, doxing, ransomware, suplantación y explotación de datos sensibles; en términos institucionales, contribuye a fortalecer la confianza en gobiernos digitales, sistemas financieros, plataformas educativas y servicios de salud; y en términos económicos, ayuda a reducir pérdidas asociadas a interrupciones, litigios, recuperación tecnológica

y sanciones regulatorias (IBM, 2024; Yar & Steinmetz, 2019). La Agenda Digital eLAC2026 reconoce esta prioridad al proponer marcos sólidos de gobernanza que resguarden privacidad, transparencia y seguridad de la información personal, lo que confirma la conveniencia regional de producir evidencia útil para política pública y gestión organizacional (CEPAL, 2024).

La viabilidad del estudio se sostiene en la disponibilidad razonable de fuentes abiertas y comparables: informes regionales, legislación vigente, documentos de autoridades de protección de datos, estrategias nacionales, reportes de incidentes y bases institucionales sobre madurez cibernética. La CEPAL ha construido matrices para 33 países de la región, mientras que el informe BID-OEA de 2025 evaluó capacidades nacionales con el modelo de madurez CMM y registró avances entre 2020 y 2025, aunque con rezagos en protección de infraestructura crítica, calidad de software e investigación en ciberseguridad (BID & OEA, 2025; CEPAL, 2024). Desde una perspectiva ética, el uso de información secundaria, agregada y pública permite minimizar riesgos para titulares de datos, siempre que se evite exponer vulnerabilidades explotables, datos personales identificables o información sensible no necesaria para el análisis (OEA, 2021; Nissenbaum, 2004).

A partir de esta brecha, el propósito del estudio es analizar la relación entre los ciberdelitos y los desafíos legales en la protección de datos personales y la privacidad digital en Latinoamérica, considerando tanto el nivel normativo como las capacidades institucionales de respuesta. Para cumplirlo, se propone describir las principales modalidades de ciberdelitos que comprometen datos personales; determinar las brechas normativas e institucionales en protección de datos, notificación de incidentes y ciberseguridad; comparar las respuestas regulatorias y operativas entre países de la región; y relacionar los costos, vectores de ataque y niveles de madurez con la existencia de mecanismos de seguridad, supervisión y cooperación. La contribución esperada consiste en ofrecer una lectura integrada, original y aplicable que conecte evidencia empírica, teoría de la privacidad y análisis jurídico comparado para orientar decisiones académicas, regulatorias y organizacionales (Acquisti et al., 2015; CEPAL, 2024; IBM, 2024; Solove, 2006).

2. Materiales y métodos

Se desarrolló una investigación documental de enfoque cualitativo, con alcance exploratorio y orientación interpretativa, adecuada para examinar un fenómeno complejo cuya comprensión exige integrar literatura científica, doctrina jurídica, reportes institucionales y marcos normativos sobre ciberdelitos, protección de datos personales y privacidad digital en Latinoamérica. La revisión bibliográfica se asumió como estrategia central porque permite ordenar conocimiento disperso, reconocer patrones conceptuales, identificar vacíos analíticos y establecer relaciones entre dimensiones jurídicas, tecnológicas e institucionales sin pretender medir causalidad estadística ni generalizar resultados poblacionales. En coherencia con ello, la unidad

de análisis estuvo conformada por publicaciones académicas, libros especializados, artículos indexados, documentos técnicos y normas vinculadas con delitos informáticos, seguridad de datos, privacidad digital, gobernanza de la ciberseguridad y responsabilidad legal frente a incidentes digitales.

Se emplearon combinaciones de términos en español, inglés y portugués, entre ellos “ciberdelitos”, “delitos informáticos”, “protección de datos personales”, “privacidad digital”, “ciberseguridad”, “phishing”, “ransomware”, “data breach”, “cybercrime”, “personal data protection”, “digital privacy” y “Latin America”. La delimitación temporal se fijó preferentemente entre 2014 y 2025, con apertura a textos clásicos cuando aportaran fundamentos teóricos indispensables para comprender la evolución conceptual de la privacidad, el delito informático o la protección jurídica de los datos personales. Esta amplitud permitió equilibrar actualidad empírica y consistencia teórica.

La selección de documentos siguió criterios de pertinencia temática, calidad académica, actualidad, trazabilidad de la fuente y relación directa con el contexto latinoamericano o con marcos conceptuales aplicables al estudio regional. Se incluyeron artículos revisados por pares, libros académicos, capítulos especializados, informes técnicos de organismos reconocidos, legislación vigente y documentos comparados sobre protección de datos, privacidad digital y respuesta institucional frente a ciberdelitos. Se excluyeron textos de opinión sin respaldo metodológico, publicaciones duplicadas, materiales sin autoría identificable, notas periodísticas no analíticas y documentos que abordaran ciberseguridad desde una perspectiva exclusivamente técnica sin conexión con protección de datos o desafíos legales. La depuración se realizó mediante lectura de título, resumen, palabras clave y texto completo, con el fin de conservar únicamente fuentes capaces de aportar evidencia, conceptos o criterios jurídicos útiles para el análisis.

El análisis se efectuó a través de una matriz de sistematización documental en la que se registraron autoría, año, país o región de referencia, tipo de fuente, objetivo del documento, enfoque metodológico, categoría jurídica abordada, modalidad de ciberdelito, dimensión de privacidad comprometida, hallazgos principales, limitaciones y aportes para la discusión. A partir de esa matriz, la información se organizó mediante codificación temática y comparación interpretativa, agrupando los resultados en ejes como modalidades de ciberdelito, vulneración de datos personales, obligaciones de seguridad, notificación de incidentes, capacidad institucional, cooperación transfronteriza, responsabilidad de actores públicos y privados, y garantías de los titulares de datos. Este procedimiento permitió reconocer convergencias, tensiones y vacíos en la literatura sin reducir el análisis a una descripción normativa aislada.

La confiabilidad del procedimiento se fortaleció mediante triangulación entre literatura científica, doctrina especializada, informes institucionales y normas aplicables, evitando depender de una sola clase de fuente para sustentar la interpretación del fenómeno. Dado que la investigación se basó en información pública y documentos

disponibles, no implicó intervención con personas, tratamiento de datos personales identificables ni acceso a sistemas informáticos, por lo que los riesgos éticos fueron mínimos. No obstante, se mantuvo especial cuidado en no reproducir información sensible, instrucciones explotables o detalles técnicos que pudieran facilitar conductas ilícitas; además, se priorizó el uso responsable de fuentes, la atribución intelectual y la lectura crítica de evidencia con sesgos potenciales. Así, la metodología permitió construir una base analítica coherente para explorar cómo los ciberdelitos tensionan la protección de datos personales y la privacidad digital en Latinoamérica.

3. Resultados

3.1. Hallazgos sobre ciberdelitos, protección de datos personales y privacidad digital en Latinoamérica

La revisión permite sostener que los ciberdelitos en Latinoamérica constituyen un fenómeno estructural de la transformación digital, no una anomalía periférica de los sistemas informáticos. La expansión de la banca digital, el comercio electrónico, la administración pública en línea, las plataformas educativas, los servicios de salud digital y las redes sociales ha incrementado el volumen de datos personales tratados por organizaciones públicas y privadas, pero esa expansión no siempre ha estado acompañada por capacidades equivalentes de prevención, supervisión, investigación y reparación. En ese sentido, la región enfrenta una paradoja: cuanto mayor es la dependencia social e institucional de los datos, mayor es también la exposición a fraudes, intrusiones, filtraciones y usos ilícitos de información personal. Este hallazgo coincide con la literatura que describe el cibercrimen como una criminalidad de oportunidad ampliada por asimetrías técnicas, debilidades regulatorias y mercados ilícitos transnacionales de datos, credenciales y accesos (Kshetri, 2013; Solove, 2006).

La evidencia regional muestra, además, que los ataques no afectan únicamente a usuarios individuales, sino también a infraestructuras organizacionales y estatales cuya interrupción puede comprometer derechos, continuidad operativa y confianza institucional. El Banco Mundial ha señalado que los incidentes cibernéticos divulgados han crecido con particular intensidad en economías emergentes, y sus análisis sobre América Latina y el Caribe advierten que la ciberseguridad se ha convertido en un componente de desarrollo económico, competitividad y resiliencia estatal, no solo en una cuestión técnica de protección de redes (Diao & Vergara Cobos, 2024). En consecuencia, los ciberdelitos deben analizarse de manera integrada con la protección de datos personales y la privacidad digital, porque el objeto final de muchos ataques no es el sistema en sí mismo, sino la extracción, manipulación, secuestro o monetización de información personal (Nissenbaum, 2004; Solove, 2006).

3.1.1. Modalidades predominantes de ciberdelitos

Las modalidades predominantes identificadas en la literatura y en los informes técnicos regionales se concentran en phishing, ransomware, robo de credenciales, malware, fraude digital, suplantación de identidad, acceso no autorizado, explotación de vulnerabilidades no corregidas y filtración de bases de datos. Esta diversidad muestra que el cibercrimen opera mediante cadenas de ataque combinadas: primero induce al error humano o explota una debilidad técnica; después obtiene acceso, privilegios o información; finalmente monetiza el daño mediante extorsión, reventa de datos, fraude financiero o interrupción deliberada de servicios. ESET reportó que en 2023 el 30% de las organizaciones latinoamericanas declaró haber sufrido al menos un incidente de seguridad, lo cual confirma que estas prácticas no son marginales, sino recurrentes en el entorno empresarial e institucional de la región (ESET, 2024; Kshetri, 2013).

El phishing destaca como una modalidad especialmente eficaz porque traslada el punto crítico de vulnerabilidad desde la infraestructura tecnológica hacia la interacción cotidiana de usuarios y trabajadores con correos, enlaces, códigos QR, formularios, aplicaciones y servicios de autenticación. IBM informó que, en Latinoamérica, el phishing representó el 16% de los incidentes de filtración de datos en 2024, con un costo promedio de US$2,91 millones por evento; a ello se suman las credenciales robadas o comprometidas, que representaron el 14% de los casos y alcanzaron un costo promedio de US$2,89 millones. Estos datos son relevantes porque evidencian que el acceso indebido no siempre requiere técnicas sofisticadas, sino que puede apoyarse en ingeniería social, contraseñas reutilizadas, autenticación débil y baja cultura de seguridad digital (IBM, 2024; Yar & Steinmetz, 2019).

El ransomware, por su parte, se consolida como una modalidad de alto impacto porque no solo compromete confidencialidad, sino también disponibilidad, continuidad del servicio y capacidad de recuperación organizacional. En la región, los ataques de ransomware han afectado empresas, instituciones públicas, proveedores tecnológicos y servicios esenciales, con consecuencias que pueden incluir paralización administrativa, pérdida de información, gastos de recuperación, pago de rescates, litigios y deterioro reputacional (Mina-Bone, 2024). La literatura especializada interpreta esta modalidad como una expresión de criminalidad digital empresarializada, en la que los atacantes operan con modelos de ransomware como servicio, negociación extorsiva y selección estratégica de víctimas con alta dependencia operativa de sus datos (Kshetri, 2013; Wall, 2007).

3.1.2. Tipos de datos personales más vulnerados

Los datos personales más vulnerados en los incidentes analizados corresponden a credenciales de acceso, nombres, documentos de identidad, direcciones físicas, correos electrónicos, números telefónicos, información financiera, historiales transaccionales, datos laborales, registros administrativos y datos asociados a servicios públicos. Esta información tiene alto valor en mercados ilícitos porque

permite construir perfiles de identidad, acceder a cuentas, realizar fraudes, solicitar créditos, ejecutar campañas de phishing personalizadas o combinar bases de datos para generar formas más sofisticadas de explotación. Desde la teoría de la privacidad, el daño no se reduce a la divulgación de un dato aislado, sino a su agregación, inferencia, reutilización y circulación fuera del contexto original de recolección (Solove, 2006; Nissenbaum, 2004).

La exposición de datos financieros y credenciales resulta particularmente crítica porque habilita pérdidas económicas inmediatas y, al mismo tiempo, daños prolongados por suplantación de identidad. Un correo electrónico combinado con número telefónico, documento de identidad, dirección y credenciales filtradas puede facilitar accesos indebidos a banca digital, billeteras electrónicas, plataformas de comercio, servicios gubernamentales y cuentas corporativas (Picoy-Gonzales et al., 2023). Por ello, los incidentes de datos deben entenderse como eventos acumulativos: una filtración aparentemente limitada puede adquirir mayor peligrosidad cuando se cruza con bases previamente expuestas, lo que incrementa el riesgo de fraude, extorsión, perfilamiento ilegal y discriminación automatizada (Acquisti et al., 2015; Solove, 2006).

Los datos sensibles constituyen una categoría de especial preocupación, sobre todo cuando se relacionan con salud, biometría, orientación, geolocalización, menores de edad, situación socioeconómica o historial educativo. En el ámbito escolar, Contreras advierte que las iniciativas regulatorias latinoamericanas enfrentan desafíos específicos respecto de los datos de niños, niñas y adolescentes, debido a que las plataformas educativas, aplicaciones institucionales y servicios digitales pueden recolectar información declarada, observada e inferida. Esta vulnerabilidad es cualitativamente distinta porque involucra sujetos con menor capacidad para comprender las consecuencias futuras del tratamiento de sus datos y porque los perfiles construidos durante la infancia pueden producir efectos persistentes en trayectorias educativas, comerciales o sociales (Contreras, 2022; Nissenbaum, 2004).

3.1.3. Principales afectaciones sociales, económicas e institucionales

Las afectaciones económicas de los ciberdelitos y las filtraciones de datos son crecientes y verificables. IBM reportó que el costo promedio de una filtración de datos en Latinoamérica alcanzó US$2,76 millones en 2024, lo que representó un aumento del 12% respecto del año anterior; además, los sectores industriales, financieros y de servicios registraron costos promedio de US$3,54 millones, US$3,22 millones y US$2,94 millones, respectivamente. Esta evidencia muestra que la inseguridad de los datos produce costos directos e indirectos: investigación forense, recuperación tecnológica, interrupción operativa, atención a usuarios afectados, defensa legal, sanciones regulatorias, pérdida de clientes y deterioro reputacional (IBM, 2024; Lehuedé, 2019).

En términos sociales, el impacto se expresa en pérdida de confianza, ansiedad digital, exposición a fraudes, hostigamiento, extorsión, daño reputacional y reducción de la

disposición ciudadana a utilizar servicios digitales. Cuando las personas perciben que sus datos pueden ser usados sin control o que las instituciones no responderán eficazmente ante incidentes, se debilita la legitimidad de la transformación digital y se amplían las brechas de inclusión (Casanova-Villalba & Casanova-Villalba, 2024). La privacidad, por tanto, no debe concebirse como un interés individual accesorio, sino como una condición de participación social, libertad informativa y autonomía en entornos mediados por datos (Acquisti et al., 2015; Nissenbaum, 2004).

En el plano institucional, los incidentes cibernéticos pueden paralizar servicios públicos, afectar recaudación fiscal, comprometer datos administrativos, interrumpir atención sanitaria, alterar trámites ciudadanos y erosionar la credibilidad del Estado. El caso de Costa Rica en 2022, citado por el Banco Mundial como un ataque de ransomware que afectó a más de veinte entidades gubernamentales, ilustra la dimensión sistémica del problema: cuando un ataque compromete plataformas estatales, el daño excede la organización afectada y se proyecta sobre derechos, servicios esenciales y gobernabilidad. La ciberseguridad se convierte así en un componente de continuidad democrática, administración pública confiable y protección efectiva de derechos fundamentales (Diao & Vergara Cobos, 2024; OEA, 2021).

3.1.4. Brechas legales en la protección de datos personales

Las brechas legales observadas en Latinoamérica no se limitan a la existencia o inexistencia de leyes, sino que abarcan el nivel de actualización normativa, la independencia de las autoridades de control, la claridad de las bases de licitud, las obligaciones de seguridad, los regímenes sancionatorios, la regulación de transferencias internacionales y los mecanismos de notificación de incidentes. La CEPAL identificó que 22 de los 33 países de América Latina y el Caribe cuentan con legislación vigente o actualizada sobre protección de datos personales, mientras que 11 carecen de una ley en la materia; esta asimetría genera una protección desigual para los titulares y dificulta la cooperación regional frente a flujos transfronterizos de datos y delitos digitales (Cabello et al., 2025; Chavarría-Mora, 2025).

La fragmentación normativa también se manifiesta en la forma en que los países regulan el consentimiento, los datos sensibles, los derechos ARCO o equivalentes, la portabilidad, la evaluación de impacto, la responsabilidad demostrada y la protección por diseño y por defecto. Chavarría-Mora observa que las leyes latinoamericanas de protección de datos muestran patrones heterogéneos de compromiso normativo, lo que implica que la región no ha alcanzado un estándar uniforme de protección comparable en todos los países. Esta heterogeneidad es problemática porque los ciberdelitos son transnacionales, mientras que las respuestas jurídicas continúan siendo predominantemente territoriales, lentas y desiguales (Chavarría-Mora, 2025; OEA, 2021).

Otro vacío relevante se vincula con la articulación entre derecho penal informático, protección de datos y regulación de ciberseguridad. En varios países, los delitos

informáticos se regulan como conductas de acceso, daño, interceptación o fraude, mientras que la protección de datos opera como régimen administrativo de tratamiento legítimo; sin embargo, los incidentes reales suelen atravesar ambas dimensiones simultáneamente. Una filtración puede involucrar acceso ilícito, incumplimiento de medidas de seguridad, falta de notificación, tratamiento indebido por terceros y responsabilidad civil o administrativa. Por ello, la ausencia de coordinación normativa dificulta una respuesta integral para investigar al atacante, sancionar negligencias organizacionales y reparar a titulares afectados (Cabello et al., 2025; Lehuedé, 2019).

3.1.5. Debilidades institucionales y técnicas para responder a incidentes

Las debilidades institucionales se observan en la limitada capacidad de detección temprana, registro de incidentes, investigación forense, cooperación internacional y coordinación entre autoridades de protección de datos, fiscalías, policías especializadas, reguladores sectoriales y equipos nacionales de respuesta. La CEPAL reportó que solo siete países de la región cuentan con CERT/CSIRT gubernamental con mandato nacional asignado por norma, mientras que doce países no poseen un CERT/CSIRT; además, dieciocho de los treinta y tres países carecen de lineamientos nacionales de notificación de incidentes. Esta situación reduce la visibilidad del problema, impide construir estadísticas sólidas y retrasa la contención de ataques que podrían escalar rápidamente entre instituciones interconectadas (Cabello et al., 2025).

En el nivel organizacional, la preparación técnica sigue siendo desigual. ESET informó que solo el 52% de las organizaciones latinoamericanas implementa planes de respuesta ante incidentes, el 46% cuenta con planes de continuidad de negocio, el 30% dispone de soluciones de prevención de pérdida de datos y apenas el 18% utiliza inteligencia de amenazas. Estos porcentajes revelan una brecha entre la conciencia del riesgo y la implementación efectiva de controles, especialmente en organizaciones que dependen intensamente de datos personales, pero carecen de presupuestos, talento especializado o marcos de gobernanza suficientemente maduros (ESET, 2024; Lehuedé, 2019).

La capacitación del personal emerge como una debilidad transversal, pues muchas intrusiones comienzan con errores humanos inducidos por ingeniería social, enlaces maliciosos o solicitudes fraudulentas de credenciales. La baja alfabetización en ciberseguridad no debe atribuirse únicamente a los usuarios, sino a modelos organizacionales que delegan la protección en decisiones individuales sin ofrecer formación continua, autenticación robusta, controles de acceso, simulaciones, protocolos claros y canales seguros de reporte (Hurtado-Guevara & Casanova-Villalba, 2022). En consecuencia, la resiliencia institucional depende menos de herramientas aisladas y más de una arquitectura de prevención que combine tecnología, cultura organizacional, liderazgo, auditoría y responsabilidad demostrable (IBM, 2024; OEA, 2021).

3.1.6. Relación entre privacidad digital y gobernanza de la ciberseguridad

El hallazgo integrador es que privacidad digital y gobernanza de la ciberseguridad no pueden tratarse como agendas separadas. La privacidad establece límites, principios y derechos frente al tratamiento de datos personales; la ciberseguridad aporta controles, capacidades y procedimientos para preservar confidencialidad, integridad y disponibilidad; y la gobernanza articula responsabilidades, rendición de cuentas, recursos, supervisión y toma de decisiones. Cuando estas dimensiones se gestionan de manera fragmentada, las organizaciones pueden cumplir formalmente una norma de privacidad, pero carecer de capacidad real para prevenir o contener incidentes; o pueden invertir en seguridad técnica sin respetar principios de minimización, finalidad, transparencia y proporcionalidad (Nissenbaum, 2004; Solove, 2006).

La gobernanza de la ciberseguridad orientada a la protección de datos exige incorporar evaluaciones de riesgo, análisis de impacto, privacidad desde el diseño, privacidad por defecto, gestión de terceros, clasificación de información, notificación oportuna de incidentes, continuidad operativa y métricas verificables de madurez. Los Principios Actualizados de la OEA sobre privacidad y protección de datos personales destacan la importancia de responsabilidad, seguridad, transparencia y tutela efectiva, mientras que los informes de CEPAL subrayan la necesidad de construir ecosistemas de confianza digital en los que la protección de datos y la ciberseguridad operen de manera coordinada. Esta convergencia es indispensable para que la digitalización regional no derive en mayor exposición de los ciudadanos, sino en servicios más confiables, inclusivos y respetuosos de derechos (OEA, 2021; Cabello et al., 2025).

Finalmente, la relación entre privacidad y gobernanza redefine la responsabilidad de empresas e instituciones públicas: la protección de datos deja de ser una obligación meramente documental y se convierte en una práctica de dirección estratégica. Lehuedé sostiene que la gobernanza corporativa en América Latina y el Caribe debe asumir la protección de datos como parte de la gestión de riesgos y de la responsabilidad de directorios y alta gerencia; ello implica pasar de una lógica reactiva centrada en cumplimiento mínimo a una lógica preventiva basada en responsabilidad demostrada, supervisión continua y cultura organizacional. La originalidad del enfoque para el artículo radica precisamente en conectar modalidades delictivas, datos vulnerados, impactos, brechas legales, debilidades institucionales y gobernanza, mostrando que la privacidad digital solo es efectiva cuando se integra con capacidades reales de ciberseguridad y con marcos jurídicos aplicables (Lehuedé, 2019; Chavarría-Mora, 2025).

4. Discusión

El conjunto de hallazgos confirma que los ciberdelitos en Latinoamérica no deben interpretarse como incidentes tecnológicos aislados, sino como manifestaciones de una vulnerabilidad estructural asociada a la digitalización acelerada, la expansión de

servicios basados en datos y la desigual madurez institucional de la región. La evidencia revisada muestra que la protección de datos personales y la privacidad digital se encuentran tensionadas por una criminalidad transnacional que aprovecha la fragmentación normativa, la baja cultura de seguridad y la limitada capacidad de respuesta estatal y organizacional. Esta lectura coincide con los análisis que ubican la ciberseguridad como condición habilitante del desarrollo digital, pues la confianza en plataformas públicas y privadas depende de que los datos sean tratados con seguridad, legalidad, proporcionalidad y responsabilidad demostrable (Cabello et al., 2025; Diao & Vergara Cobos, 2024; Kshetri, 2013).

Los resultados relativos a las modalidades predominantes de ciberdelitos sugieren que la amenaza regional opera mediante una combinación de sofisticación técnica y explotación de vulnerabilidades ordinarias. El phishing, el ransomware, el robo de credenciales, el malware, la suplantación de identidad y la explotación de fallas no corregidas aparecen como prácticas recurrentes porque se apoyan en factores humanos, deficiencias organizacionales y oportunidades de monetización rápida. El hecho de que ESET haya reportado que el 30% de las organizaciones latinoamericanas sufrió al menos un incidente de seguridad en 2023, y que IBM haya identificado el phishing como el vector inicial más frecuente en filtraciones regionales de 2024, permite sostener que el problema no se reduce a ataques excepcionales, sino a patrones persistentes de exposición digital (ESET, 2024; IBM, 2024; Yar & Steinmetz, 2019).

La discusión adquiere mayor densidad cuando se observa que el ciberdelito contemporáneo no solo busca acceder a sistemas, sino capturar, combinar y revender datos personales. Desde esta perspectiva, las credenciales, documentos de identidad, correos, teléfonos, direcciones, datos bancarios, registros administrativos, información laboral, datos de salud y datos de menores adquieren valor ilícito porque pueden reutilizarse para fraude, extorsión, perfilamiento, discriminación o ingeniería social dirigida. La taxonomía de Solove permite comprender que el daño a la privacidad no se limita a la divulgación, sino que incluye agregación, inseguridad, uso secundario e intrusión; a su vez, Nissenbaum enfatiza que la privacidad se vulnera cuando la información fluye fuera de las normas del contexto en que fue entregada (Nissenbaum, 2004; Solove, 2006).

Las afectaciones económicas e institucionales refuerzan la necesidad de tratar estos hallazgos como un problema de gobernanza y no solo de cumplimiento técnico. IBM informó que el costo promedio de una filtración de datos en Latinoamérica alcanzó US$2,76 millones en 2024, con incrementos relevantes en sectores industrial, financiero y de servicios; además, las filtraciones asociadas a múltiples entornos de almacenamiento y a credenciales comprometidas evidencian que la complejidad tecnológica eleva los costos de contención y recuperación. Estas cifras son consistentes con la literatura que advierte que la privacidad tiene una dimensión económica y conductual: las personas, organizaciones e instituciones suelen subestimar riesgos futuros, aun cuando las consecuencias de una exposición de datos

pueden ser acumulativas, duraderas y socialmente costosas (Acquisti et al., 2015; IBM, 2024; Lehuedé, 2019).

Las brechas legales identificadas muestran que la región ha avanzado en el reconocimiento formal de la protección de datos personales, pero todavía enfrenta dificultades para convertir ese reconocimiento en tutela efectiva. La CEPAL reporta que 22 de los 33 países de América Latina y el Caribe cuentan con legislación vigente o actualizada en protección de datos personales, mientras que 11 carecen de una ley específica; además, la existencia de autoridades de control no garantiza por sí misma capacidad sancionatoria, independencia, cooperación transfronteriza ni articulación con fiscalías, CERT/CSIRT y reguladores sectoriales. Por ello, la heterogeneidad normativa descrita por Chavarría-Mora resulta especialmente problemática: los datos circulan regional y globalmente, mientras las garantías, obligaciones y mecanismos de respuesta continúan anclados en marcos nacionales desiguales (Cabello et al., 2025; Chavarría-Mora, 2025; Organización de los Estados Americanos [OEA], 2021).

Las debilidades institucionales y técnicas también permiten explicar por qué los incidentes escalan con rapidez y por qué muchas organizaciones reaccionan de manera tardía. La ausencia de lineamientos nacionales de notificación de incidentes en una parte importante de los países, junto con la disponibilidad desigual de CERT/CSIRT con mandato nacional, limita la trazabilidad de los ataques, reduce la calidad de las estadísticas públicas y dificulta la coordinación entre actores. En el plano organizacional, la baja adopción de planes de respuesta, continuidad de negocio, prevención de pérdida de datos e inteligencia de amenazas revela que la región aún opera con una lógica reactiva, más centrada en remediar daños que en prevenirlos mediante arquitectura institucional, formación permanente y responsabilidad demostrable (Cabello et al., 2025; ESET, 2024; IBM, 2024).

La relación entre privacidad digital y gobernanza de la ciberseguridad constituye el eje interpretativo más relevante de la discusión. La privacidad define principios, límites y derechos sobre el tratamiento de datos; la ciberseguridad provee mecanismos para preservar confidencialidad, integridad y disponibilidad; y la gobernanza permite asignar responsabilidades, recursos, controles y rendición de cuentas. Cuando estas dimensiones se administran por separado, las organizaciones pueden exhibir políticas de privacidad formalmente correctas, pero carecer de medidas reales para impedir accesos indebidos; o, en sentido inverso, pueden desplegar controles técnicos sin respetar minimización, finalidad, transparencia y proporcionalidad. De ahí que la protección de datos por diseño, la evaluación de impacto, la notificación de incidentes y la gestión de terceros deban entenderse como componentes de una misma arquitectura de confianza digital (Cabello et al., 2025; Lehuedé, 2019; OEA, 2021).

El análisis también permite discutir una tensión crítica: el consentimiento, aunque central en la protección de datos, resulta insuficiente cuando los titulares enfrentan ecosistemas digitales opacos, asimetrías informativas y cadenas de tratamiento difíciles de comprender. En contextos de phishing, aplicaciones interconectadas,

servicios en la nube, publicidad comportamental y plataformas educativas, el usuario no siempre puede anticipar la circulación futura de su información ni evaluar adecuadamente los riesgos derivados de su reutilización. Por ello, la literatura contemporánea sobre privacidad advierte que la autonomía informativa requiere algo más que aceptación contractual: exige diseño institucional, límites sustantivos al tratamiento, supervisión independiente y obligaciones preventivas para quienes recolectan, procesan o comparten datos personales (Acquisti et al., 2015; Contreras, 2022; Nissenbaum, 2004).

En términos prácticos, los hallazgos sugieren que la respuesta regional debe avanzar hacia un modelo de convergencia regulatoria y operativa. No basta con tipificar delitos informáticos ni con aprobar leyes de protección de datos si estas no dialogan con políticas de ciberseguridad, capacidades forenses, cooperación internacional, cultura organizacional y mecanismos de reparación a titulares afectados. La armonización de estándares mínimos, la obligatoriedad de notificar incidentes, el fortalecimiento de autoridades de control, la profesionalización de equipos de respuesta y la incorporación de métricas de madurez permitirían reducir la brecha entre norma y práctica. Esta orientación es consistente con los Principios Actualizados de la OEA, que proponen seguridad, transparencia, responsabilidad y tutela efectiva como ejes para fortalecer los marcos nacionales de protección de datos (OEA, 2021; Cabello et al., 2025; Chavarría-Mora, 2025).

La contribución del artículo radica en articular dimensiones que con frecuencia se estudian de forma separada: modalidades de ciberdelito, tipos de datos vulnerados, impactos económicos e institucionales, brechas legales, debilidades técnicas y gobernanza de la privacidad. Esta integración permite sostener que la protección de datos personales en Latinoamérica no puede depender exclusivamente de reformas normativas ni de soluciones tecnológicas aisladas, sino de ecosistemas de confianza capaces de prevenir, detectar, contener, sancionar y reparar daños. Al tratarse de una revisión bibliográfica exploratoria, la discusión no pretende establecer causalidades definitivas, pero sí delimitar un marco interpretativo sólido para investigaciones posteriores comparativas, estudios empíricos por país y evaluaciones sectoriales de madurez en ciberseguridad y privacidad digital (Cabello et al., 2025; Diao & Vergara Cobos, 2024; Solove, 2006).

5. Conclusiones

Los hallazgos permiten concluir que los ciberdelitos en Latinoamérica constituyen un problema jurídico, institucional y social de alta complejidad, debido a que no se limitan a la vulneración de sistemas informáticos, sino que comprometen directamente la protección de datos personales, la privacidad digital, la confianza ciudadana y la continuidad de servicios esenciales. En este sentido, el fenómeno exige una lectura integral que supere la visión técnica del riesgo y reconozca que cada incidente digital

puede derivar en afectaciones económicas, reputacionales, legales y sociales de amplio alcance.

Se concluye que las modalidades predominantes de ciberdelitos, especialmente el phishing, el ransomware, el robo de credenciales, la suplantación de identidad, el acceso no autorizado y la filtración de bases de datos, evidencian una criminalidad digital cada vez más organizada, adaptable y transnacional. Estas prácticas aprovechan vulnerabilidades tecnológicas, fallas normativas, insuficiente capacitación de usuarios y debilidades organizacionales, lo que demuestra que la prevención no puede depender únicamente de herramientas informáticas, sino de políticas sostenidas de gestión del riesgo, formación y responsabilidad institucional.

Asimismo, se establece que los datos personales más vulnerados poseen un valor estratégico para los actores ilícitos, especialmente cuando incluyen información financiera, documentos de identidad, credenciales, datos de contacto, registros administrativos, datos de salud, información de menores y perfiles digitales. La exposición de estos datos no produce daños aislados, sino riesgos acumulativos, porque la información filtrada puede reutilizarse en fraudes posteriores, extorsiones, perfilamientos ilegales, accesos indebidos y nuevas formas de manipulación digital.

Otra conclusión relevante es que las afectaciones de los ciberdelitos trascienden el plano individual y alcanzan dimensiones económicas e institucionales significativas. Las filtraciones de datos generan costos de recuperación, interrupción operativa, pérdida de clientes, deterioro reputacional, sanciones, litigios y reducción de la confianza en servicios digitales. En el ámbito público, los ataques pueden comprometer trámites, plataformas estatales, servicios esenciales y mecanismos de gobernabilidad, lo que convierte la ciberseguridad en una condición indispensable para la estabilidad institucional y la protección efectiva de derechos.

Se concluye también que Latinoamérica presenta avances normativos importantes en materia de protección de datos personales, pero estos progresos siguen siendo desiguales, fragmentados y, en varios casos, insuficientes frente a la velocidad de los ciberdelitos. La existencia de leyes y autoridades de control no garantiza por sí misma una tutela efectiva si no existen mecanismos claros de notificación de incidentes, cooperación transfronteriza, sanciones proporcionales, independencia regulatoria, capacidades forenses y coordinación entre instituciones responsables de seguridad digital, justicia y protección de datos.

Finalmente, el análisis permite afirmar que la privacidad digital solo puede protegerse de manera efectiva cuando se articula con una gobernanza sólida de la ciberseguridad. Esto implica integrar principios jurídicos, medidas técnicas, cultura organizacional, responsabilidad de directivos, gestión de terceros, evaluación de riesgos, transparencia y respuesta oportuna ante incidentes. La principal contribución del estudio radica en mostrar que los desafíos legales de la protección de datos personales en Latinoamérica no pueden resolverse mediante normas aisladas ni soluciones tecnológicas parciales, sino mediante un ecosistema de confianza digital

capaz de prevenir, detectar, contener, sancionar y reparar los daños derivados de la criminalidad informática.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Arcos-Chaparro, I. A., & Epia-Silva, M. A. (2024). La transverzalización del debido proceso en las relaciones laborales particulares. *Journal of Economic and Social Science Research*, *4*(2), 17–43. https://doi.org/10.55813/gaea/jessr/v4/n2/100

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2025). *2025 Cybersecurity Report: Vulnerability and maturity challenges to bridging the gaps in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2025-Cybersecurity-Report-Vulnerability-and-Maturity-Challenges-to-Bridging-the-Gaps-in-Latin-America-and-the-Caribbean.pdf

Barahona-Martinez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), 46–64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, *1*(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Bonilla-Morejón, D. M. (2023). Derecho Penal y Políticas de Seguridad en Ecuador: Análisis de la Eficacia. *Revista Científica Zambos*, *2*(3), 59-74. https://doi.org/10.69484/rcz/v2/n3/50

Cabello, S. M., Fernández, M., Elaskar, M., Pallero, M., Pereira, F., Ros Rooney, D., & Urtasun, M. (2025). *Construcción de un ecosistema de confianza y seguridad digital*. Comisión Económica para América Latina y el Caribe. https://repositorio.cepal.org/bitstreams/a719d213-00b5-4534-91c3-2d70bf232dd9/download

Casanova-Villalba, C. I. y Casanova-Villalba, L. A. (2024). Uso de análisis de datos avanzados para la detección de fraudes financieros. *Revista Científica Ciencia y Método, 2*(3), 1–12. https://doi.org/10.55813/gaea/rcym/v2/n3/44

Chavarría-Mora, E. (2025). (Lack of) patterns in commitment: Data protection in the Latin America and Caribbean personal data protection laws. *Social Media + Society, 11*(2). https://doi.org/10.1177/20563051251337206

Comisión Económica para América Latina y el Caribe. (2024). *Agenda digital para América Latina y el Caribe (eLAC2026)*. https://www.cepal.org/es/publicaciones/80860-agenda-digital-america-latina-caribe-elac2026

Comisión Económica para América Latina y el Caribe. (2024). *Construcción de un ecosistema de confianza y seguridad digital*. https://repositorio.cepal.org/bitstreams/a719d213-00b5-4534-91c3-2d70bf232dd9/download

Contreras, A. (2022). Regulatory initiatives on school children's data protection in Latin America. *Revista Latinoamericana de Economía y Sociedad Digital, 3*. https://doi.org/10.53857/RAKT3016

Diao, H., & Vergara Cobos, E. (2024). *Cybersecurity economics for Latin America and the Caribbean*. World Bank. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P179481-5515e6c4-1d69-444d-a057-741edce07402.pdf

ESET. (2024). *ESET Security Report 2024*. https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-2024-es.pdf

García Moreno, M., & Vargas Fonseca, A. D. (2023). Restitución de derechos territoriales y ordenamiento ambiental en territorios étnicos en Colombia. *Journal of Economic and Social Science Research*, *3*(3), 76–96. https://doi.org/10.55813/gaea/jessr/v3/n3/74

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. J. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hurtado-Guevara, R. F. y Casanova-Villalba, C. I. (2022). La auditoría forense como herramienta para la detección de fraudes financieros en Ecuador. *Revista Científica Zambos, 1*(1), 33–50. https://doi.org/10.69484/rcz/v1/n1/52

IBM. (2024). *Cost of a Data Breach Report 2024*. IBM Security. https://www.ibm.com/reports/data-breach

Kshetri, N. (2013). Cybercrime and cybersecurity in Latin American and Caribbean economies. En *Cybercrime and cybersecurity in the Global South* (pp. 135–151). Palgrave Macmillan. https://doi.org/10.1057/9781137021946_7

Lehuedé, H. J. (2019). *Corporate governance and data protection in Latin America and the Caribbean*. Comisión Económica para América Latina y el Caribe. https://www.cepal.org/es/node/49380

Mendoza-Armijos, H. E., Camacho-Medina, B. M., & García-Segarra, H. G. (2023). Análisis de la justicia restaurativa como alternativa al sistema penal tradicional en América Latina. *Revista Científica Ciencia Y Método, 1*(3), 58-69. https://doi.org/10.55813/gaea/rcym/v1/n3/20

Mina-Bone, S. G. (2024). Evolución del derecho penal económico frente a los delitos financieros digitales. *Revista Científica Ciencia y Método, 2*(3), 52–66. https://doi.org/10.55813/gaea/rcym/v2/n3/50

Moscoso-Loayza, E., Anrrango-Mesa, E. R., Torres-Ortiz, J. V., Encalada-Echeverría, A. L., Landázuri-Pastrana, F. J., Lopez-Salinas, C. M., & Andachi-Trujillo, W. A. (2024). *Corrupción y Narcotráfico: Implicaciones del Derecho Penal en la Lucha contra la Corrupción Sistémica en Latinoamérica.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.104

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Núñez-Ribadeneyra, R. A. (2023). Derechos Humanos y Justicia Social en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 42-58. https://doi.org/10.69484/rcz/v2/n3/49

Organización de los Estados Americanos. (2021). *Updated principles on privacy and personal data protection*. https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H. y Omonte-Vilca, A. (2023). *Fortalecimiento metodológico de la seguridad informática en posgrados: Análisis y estrategias de mejora*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.56

Pita-Arizaga, A. E. (2024). Integración de la perspectiva de género en la jurisprudencia constitucional latinoamericana. *Revista Científica Ciencia Y Método, 2*(4), 14-25. https://doi.org/10.55813/gaea/rcym/v2/n4/49

Samaniego-Quiguiri, D. P. (2023). Acceso a la Justicia y Equidad en el Sistema Legal Ecuatoriano. *Revista Científica Zambos*, *2*(2), 50-62. https://doi.org/10.69484/rcz/v2/n2/45

Samaniego-Quiguiri, D. P., & Bonilla-Morejón, D. M. . (2024). Análisis de la Evolución del Derecho Constitucional en Ecuador: Implicaciones para el Desarrollo Democrático. *Revista Científica Zambos, 3*(3), 1-14. https://doi.org/10.69484/rcz/v3/n3/53

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1066922

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE. https://books.google.com/books/about/Cybercrime_and_Society.html?id=_nN7DwAAQBAJ