ORIGINAL
Artículo de Investigación

Variables asociadas a los delitos informáticos en Latinoamérica*

Variables associated with cybercrime in Latin America

Recibido: Junio 20 de 2023 – Evaluado: Agosto 22 de 2023 - Aceptado: Septiembre 22 de 2023

Rolando Eslava-Zapata**
Carlos Julio Rojas-Hermida***
John Edisson García-Peñaloza****

Para citar este artículo/ To cite this article

Eslava-Zapata, R., Rojas-Hermida, C. J., & García-Peñaloza, J. E. (2024). Variables asociadas a los delitos informáticos en Latinoamérica. *Revista Academia & Derecho, 15*(28), 1-21.

Resumen
El objetivo del estudio es analizar las variables asociadas a los delitos informáticos en Latinoamérica. El estudio es de tipo cuantitativo con un diseño transeccional. Al respecto, se trabaja con la base de datos del Observatorio de Delitos Informáticos de Latinoamérica (ODILA) del periodo 2015-2017, con una muestra conformada por 5310 personas. Los resultados revelan que de la relación de la denuncia por país y el sexo, el sexo masculino tiene su presencia total en Argentina. Mientras que la distribución del sexo femenino tiene mayor presencia en México

* Artículo inédito. Artículo de investigación e innovación. Artículo de investigación. Trabajo vinculado a proyecto de la Universidad Libre Colombia Seccional Cúcuta.

** Doctor en Administración por la Universidad Complutense de Madrid, España. Profesor-Investigador de la Universidad Libre Colombia Seccional Cúcuta, Colombia. Correo electrónico: rolandoa.eslavaz@unilibre.edu.co ORCID: https://orcid.org/0000-0003-1459-9600

*** Magister en Negocios Internacionales por la Universidad EAN. Profesor-Investigador de la Universidad Surcolombiana, Colombia. Correo electrónico: carlosjulio.rojas@usco.edu.co ORCID: https://orcid.org/0000-0003-1459-9600

**** Magister en Administración de Empresas por la EUDE Business School, España. Profesor-Investigador de la Corporación Unificada Nacional de Educación Superior, Colombia. Correo electrónico: john_garciape@cun.edu.co ORCID: https://orcid.org/0000-0003-3788-0411

(22,38%), Colombia (20,23%) y Guatemala (8,54%). También se evidencia que de relación del nivel de instrucción y si ha denunciado, un alto porcentaje de los que no han denunciado tienen nivel universitario (81,35%). En cuanto a la relación entre el incidente y el tipo de víctima, se encuentra que las personas físicas son las que más denuncian los delitos informáticos, sobre todo, en delitos como calumnias e injurias (17,30%), amenazas (15,97%) y hacking (15,12%). Además, de la relación entre las causas por las cuales no denunció y la edad, se deriva que las personas con edad entre 22 y 35 son las que más participación tienen del grupo de estudio. Se concluye que los delitos informáticos atentan contra la privacidad de las personas y organizaciones. Los ciberdelincuentes han encontrado un espacio para el enriquecimiento ilícito, el robo de información y desestabilización de la integridad de los afectados. Las organizaciones están recurriendo a la auditoría a fin de lograr obtener pruebas ante procesos judiciales, puesto que la auditoría permite la detección de los delitos informáticos y la creación de dispositivos que protejan a las organizaciones de injerencias de extraños que atenten contra el capital y la reputación.
Palabras Clave: Delito Informático, Ciberdelito, Denuncia, Victima, Incidente.

Abstract
The objective of this study is to analyze the variables associated with computer-related crime in Latin America. The study is quantitative with a cross-sectional design. In this regard, we work with the database of the Observatory of Computer Crimes in Latin America (ODILA) for the period 2015-2017, with a sample of 5310 people. The results reveal that from the relationship of the complaint by country and sex, the male sex has its total presence in Argentina. The distribution of the female sex has a greater presence in Mexico (22.38%), Colombia (20.23%), and Guatemala (8.54%). It is also evident that a high percentage of those who have not reported the incident have a university level of education (81.35%). As for the relationship between the incident and the type of victim, it is found that individuals are the most likely to report computer crimes, especially in crimes such as slander and libel (17.30%), threats (15.97%), and hacking (15.12%). Furthermore, from the relationship between the reasons for not reporting and age, it can be seen that people aged between 22 and 35 are the ones with the highest participation in the study group. It is concluded that cybercrime threatens the privacy of individuals and organizations. Cybercriminals have found a space for illicit enrichment, information theft, and destabilization of the integrity of those affected. Organizations are resorting to auditing in order to obtain evidence in legal proceedings since auditing allows the detection of computer crimes and the creation of devices that protect organizations from interference by outsiders who threaten their capital and reputation.
Keywords: Computer Crime, Cybercrime, Reporting, Victim, Incident.

Resumo
O objetivo deste estudo é analisar as variáveis associadas ao crime cibernético na América Latina. O estudo é quantitativo e tem um desenho de corte transversal. Nesse sentido, trabalhamos com o banco de dados do Observatório de Crimes Informáticos da América Latina (ODILA) para o período de 2015 a 2017, com uma amostra de 5.310 pessoas. Os resultados revelam que, em termos de denúncias por país e sexo, o sexo masculino tem uma presença total na Argentina. Já a distribuição do sexo feminino tem maior presença no México (22,38%), Colômbia (20,23%) e

Guatemala (8,54%). Também é evidente que uma alta porcentagem dos que não relataram o incidente tem nível universitário de educação (81,35%). Quanto à relação entre o incidente e o tipo de vítima, verifica-se que as pessoas físicas são as que mais denunciam crimes relacionados a computadores, especialmente crimes como calúnia e difamação (17,30%), ameaças (15,97%) e hacking (15,12%). Além disso, a relação entre os motivos para não denunciar e a idade mostra que as pessoas com idade entre 22 e 35 anos são as mais propensas a se envolver no grupo de estudo. Conclui-se que o crime cibernético viola a privacidade de indivíduos e organizações. Os criminosos cibernéticos encontraram um espaço para enriquecimento ilícito, roubo de informações e desestabilização da integridade das pessoas afetadas. As organizações estão recorrendo à auditoria para obter provas em processos judiciais, pois a auditoria permite a detecção de crimes cibernéticos e a criação de mecanismos para proteger as organizações da interferência de pessoas de fora que ameaçam o capital e a reputação.
Palavras-chave: Crime de computador, crime cibernético, reclamação, vítima, incidente.

Résumé
L'objectif de cette étude est d'analyser les variables associées à la cybercriminalité en Amérique latine. Il s'agit d'une étude quantitative de type transversal. À cet égard, nous travaillons avec la base de données de l'Observatoire de la criminalité informatique d'Amérique latine (ODILA) pour la période 2015-2017, avec un échantillon de 5310 personnes. Les résultats révèlent qu'en termes de déclaration par pays et par sexe, le sexe masculin est totalement présent en Argentine. Le sexe féminin est plus présent au Mexique (22,38 %), en Colombie (20,23 %) et au Guatemala (8,54 %). Il est également évident qu'un pourcentage élevé de ceux qui n'ont pas signalé l'incident ont un niveau d'éducation universitaire (81,35%). En ce qui concerne la relation entre l'incident et le type de victime, on constate que ce sont les particuliers qui signalent le plus les délits informatiques, en particulier les délits tels que la diffamation (17,30 %), les menaces (15,97 %) et le piratage (15,12 %). En outre, la relation entre les motifs de non-déclaration et l'âge montre que les personnes âgées de 22 à 35 ans sont les plus susceptibles d'être impliquées dans le groupe d'étude. La conclusion est que la cybercriminalité porte atteinte à la vie privée des individus et des organisations. Les cybercriminels ont trouvé un espace pour l'enrichissement illicite, le vol d'informations et la déstabilisation de l'intégrité des personnes touchées. Les organisations se tournent vers l'audit pour obtenir des preuves dans les procédures judiciaires, car l'audit permet de détecter la cybercriminalité et de créer des mécanismes pour protéger les organisations contre l'ingérence de personnes extérieures qui menacent le capital et la réputation.
Mots-clés: Criminalité informatique, cybercriminalité, signalement, victime, incident.

SUMARIO: Introducción. - Problema de investigación. - Metodología. - Esquema de resolución de problema- Plan de redacción. – 1. Contexto de los delitos informáticos. 2. Tipos de delitos informáticos. 3. Delitos informáticos y justicia. – Plan de redacción. 1. Análisis descriptivo variables asociadas a delitos informáticos. 2. Relación entre variables asociadas a los delitos informáticos -Conclusiones. Referencias.

Introducción

En las últimas décadas los sistemas informáticos se han modernizado constantemente dinamizando las actividades económicas y sociales, permitiendo el acceso en tiempo real a una diversidad de información (Acosta, Benavides & García, 2020). La conectividad al *Internet* ha permitido a las personas entrar al mundo virtual y aprovechar los múltiples servicios ofrecidos por las organizaciones públicas o privadas sin tener que salir de casa (Villón, Sojos, Mendoza, Guarda & Clery, 2019). El desarrollo de las Tecnologías de la Información y Comunicación (TIC) han facilitado la comunicación y el intercambio de información a nivel nacional e internacional (Arcos-Argudo, Matute-Pinos & Fernández-Mora, 2023). El avance de las TIC ha supuesto un reto para los gobiernos, quienes deben estar atentos en crear normas para hacer frente a las conductas delictivas y superar las falencias a la luz de las exigencias legales y sociales en torno a los delitos informáticos y, de esta manera, velar por la protección de los ciudadanos y las organizaciones en general (Debortoli & Brignole, 2024).

A la par del avance tecnológico avanzan las formas de delinquir, puesto que ahora se usa el *Internet* para realizar actividades criminales tales como delitos sexuales, delitos contra la identidad, delitos contra la propiedad o delitos económicos y, precisamente, con la ayuda de herramientas modernas de informática se vulnera la información de las personas con el sabotaje de los sistemas y propagación de programas maliciosos, lo cual consagra la acción delictiva (Rosas-Lanas & Pila-Cárdenas, 2023).

Los Delitos Informáticos (DI) comprenden una diversidad de delitos que van desde el fraude, pasando por el *phishing* hasta llegar a crímenes racistas y xenófobos (Santana-Martínez, Romero-Zapata & Camacho-Bobadilla, 2023). Los DI son conductas que en la actualidad tienen infracción en los países y suponen consecuencias jurídicas penales (Sánchez-Díaz, 2023). Las personas y organizaciones están expuestas a los DI debido a la diversidad de operaciones que realizan por *Internet*, las cuales en muchos casos, son vulnerables a violación por los *hackers* e infección del *software* de los equipos con virus (Tamayo-Medina, Carvajal-Guerrero & Maldonado-Niño, 2023). Los DI son realizados de forma rápida y tiene la capacidad de afectar a personas de diferentes países. El mismo desarrollo tecnológico hace que el delito sea novedoso y difícil de detectar, de ahí que en algunos casos, la complejidad del delito no está tipificado en los estamentos legales existentes (Iancu, Tușa, Iancu, Simion & Moise, 2023). Aparece un nuevo bien jurídico tutelado que es la información y delitos intangibles que son difíciles de cuantificar. En este sentido, la complejidad de información y la diversidad de sistemas informáticos, hace difícil controlar a operaciones ilegales y contar con un personal capacitado que recopilen las pruebas y castiguen al delincuente (Šupa, Kaktinas & Rinkevičiūtė, 2023). Cabe destacar que la información como bien jurídico tutelado debe verse de forma amplia, porque abarca documentos, bases de datos, información bancaria o médica, información empresarial, entre otros (Guatemala-Mariano & Martínez-Prats, 2023).

Los ordenamientos jurídicos en Latinoamérica tienen diferentes definiciones sobre los DI, pero lo que debe quedar claro, es que los DI son actos ilícitos penales que causan daños económicos o morales a personas naturales o jurídicas (Rodríguez-Ayuso, 2021). Los ciberdelincuentes violan los sistemas de seguridad informáticos y vulneran la información de terceros a cambios de

benéficos personales. Por lo tanto, los DI abarcan el daño de equipos de computación, redes de *Internet* y medios electrónicos (Santacruz & Hermoza, 2019).
En este sentido, conocer las variables relacionadas con los delitos informáticos permite a los organismos de seguridad enfrentar las consecuencias personales de las víctimas (Alcívar-Trejo, Blanc-Pihuave & Calderón-Cisneros, 2018). En avance de la informática ha venido acompañada de riegos para las personas y organizaciones públicas o privadas quienes están vulnerables ante los delincuentes informáticos quienes roban información y hacen actividades fraudulentas (Eslava-Zapata, Omaña-Guerrero, Sierra-Narváez & Mogrovejo-Andrade, 2023).
La investigación tuvo por objetivo analizar las variables asociadas a los delitos informáticos en Latinoamérica. El estudio es de tipo cuantitativo con un diseño transeccional. Al respecto, se trabajó con la base de datos del Observatorio de Delitos Informáticos de Latinoamérica (ODILA) del periodo 2015-2017, con una muestra conformada por 5310 personas.

Problema de investigación

¿Qué variables están asociadas a los delitos informáticos en Latinoamérica?

Metodología

El estudio es de tipo cuantitativo con un diseño transeccional, dado que se describió el comportamiento de las variables asociadas a los delitos informáticos (Hernández-Sampieri, Fernández-Collado & Baptista-Lucio, 2014). Al respecto, se trabajó con la base de datos del Observatorio de Delitos Informáticos de Latinoamérica (ODILA), con una muestra conformada por 5310 personas distribuidas de la siguiente manera: 1290 personas en 2015, 1260 personas en 2016 y 2760 personas en 2017 (Observatorio de Delitos Informáticos de Latinoamérica, 2015, 2016, 2017).
Las variables asociadas a los delitos informáticos analizadas corresponden a: denuncia por país, tipo de víctima, edad, sexo, nivel de instrucción, ha denunciado, causas por las que no denunció, incidente y correo electrónico. Al respecto apoyados en el programa Excel de Microsoft Office y el *Statistical Package for the Social Sciences* (SPSS), se realizó el análisis descriptivo de las variables asociadas a los delitos informáticos por año y las relaciones entre algunas de ellas (Eslava-Zapata, Ferney-Archila, Mogrovejo-Andrade, Chacón-Guerrero & Esteban-Montilla, 2024).

Esquema de resolución del problema de investigación

Para dar respuesta a la pregunta de investigación el trabajo se dividió en dos partes perfectamente diferenciadas. La primera parte aborda algunos aspectos teóricos relacionados con los delitos informáticos y la segunda parte corresponde al análisis de la base de datos de ODILA.

Plan de redacción

1. **Contexto de los delitos informáticos**

Las organizaciones ante los avances de la informática están ofreciendo una diversidad de servicios para comunicarse con las personas. en la actualidad existe la posibilidad de acceder a una extensa cantidad de contenidos documentos, videos, portales, entre otras, que facilitan la interacción sin límites de edad, sexo o estatus social (Blázquez-Agudo, 2021). El acceso a gran cantidad de datos sensibles y personales de forma sencilla ha abierto una oportunidad para los delincuentes informáticos quienes violan los sistemas de seguridad y ponen en riesgo la integridad de las personas. los ciberdelincuentes convierten en blanco las personas y organizaciones a fin de enriquecerse (Fakiha, 2023).

Los DI son aquellos comportamientos ilegales y antiéticos que generan daños a terceros como robo de datos o pérdida de bienes jurídicos que suceden en el ciberespacio que deben ser tratados legalmente (de-la-Garza-Montemayor & Leal-Espinoza, 2020). Los DI también son conocidos como delitos telemáticos, cibercrimen, entre otros; lo que debe quedar claro es que estas conductas criminales amenazan la privacidad y provocan daños patrimoniales en personas y organizaciones (Subanjui, Wattanakomol & Silpcharu, 2023).

Por lo expuesto, los entes gubernamentales en los países latinoamericanos están desarrollando programas de seguridad y normas que protejan la privacidad de los ciudadanos y controlar los riesgos de seguridad, integridad y acceso a la información (Mejía-Lobo, Hurtado-Gil & Grisales-Aguirre, 2023). Existe una necesidad por reglamentar los DI a nivel nacional e internacional con alcance global de cara a proteger la información y salvaguardar el bien jurídico, con ello, el aparato jurídico tiene herramientas legales para castigar las conductas punibles (Mattace, 2024).

Considerando el espectro territorial de los DI, que en la actualidad traspasan las fronteras de las naciones, exige una armonización de la legislación de cara a una cooperación internacional efectiva como lo establece el Convenio de Budapest (Fernández & Vargas, 2018); sin lugar a dudas, esto facilitaría la obtención adecuada de evidencias que pueden ser preservadas de forma digital, la cual reviste de vital importancia para el esclarecimiento del proceso penal; asimismo, se estandarizarían los procedimientos y normas, para usar el mismo lenguaje en la comprensión de los DI (Linares, 2020).

2. Tipos de delitos informáticos

El avance de las tecnologías, el uso del *Internet*, equipos de computación y dispositivos móviles, ha fomentado la práctica digital en las personas para resolver actividades laborales o personales. Se han identificado diferentes modalidades de DI, entre ellas se encuentran:

- Acceso no autorizado: es la violación de los sistemas de seguridad llevada a cabo por los hackers.
- Intercepción no autorizada: riesgo en el acceso al control de los programas.
- Daño a programas informáticos: deterioro de los programas informáticos para evitar el acceso a la información.

- Sabotaje informático: eliminación de los programas informáticos para evitar su funcionamiento. Un ejemplo de este tipo de delitos son los virus que se crean para infectar archivos y programas.
- Espionaje informático: es la adquisición de información confidencial a fin de tener ganancias metálicas. El robo de proyectos industriales y datos personales, son delitos muy característicos, que ponen en riesgo la filtración de información y la identidad.

Por otra parte, el Consejo Europeo (2001, 2008) identificó como DI los siguientes:

- Acceso e interferencia de sistemas informáticos.
- Intercepción ilícita de datos informáticos.
- Falsificación y fraude informático.
- Producción o adquisición de contenido pornográfico infantil.
- Infracción de la propiedad intelectual.
- Difusión de material xenófobo o racista.
- Insultos o amenazas xenófobas o racistas.

En el caso colombiano la Ley 1273 de 2009 establece como DI:

- Obstaculización ilegitima de sistema informático.
- Interceptación de daños informáticos.
- Daños informáticos.
- Uso de software malicioso.
- Violación de datos personales.
- Hurtos de medios informáticos.
- Transferencia no consentida de activos.

3. Delitos informáticos y justicia

Se ha demostrado la falta de castigo de los DI debido a los vacíos legales existentes, los cuales son aprovechados por los delincuentes por los delincuentes, que amenazan la estabilidad económica de las personas y organizaciones (Vázquez-Cano & Pascual -Moscoso, 2022). De ahí que la preocupación de gobiernos y entes gubernamentales internacionales para tomar medidas que permitan contrarrestar este flagelo, proteger a la población y castigar a los criminales (Gascón-Marcén, 2021).

Una de las prácticas más comunes en la solución de los DI es la ciencia forense. La ciencia forense digital utilizando herramientas avanzadas de software y hardware busca evidencias del DI en las fuentes digitales (Stratonov, Slinko & Slinko, 2021). El avance de herramientas cada vez más sofisticadas para la detección de DI, demandará un cuerpo policial competente que fomente un ciberespacio seguro (Guerrero-Guerrero, 2020).

Los DI se han hecho frecuentes en Latinoamérica lo que confirma el carácter transnacional de estos y las amenazas provenientes tanto del interior del país como de otros países (Graves & Acquisti,

2023). Existen diversos incidentes que pueden afectar la fuga de información confidencial, por ejemplo, los desastres naturales que afectan el ciberespacio, el espionaje para sustraer o sabotear información confidencial y el uso de dispositivos infectados con programas maliciosos (Navarro-Dolmestch, 2023). Las normas existentes regulan y tipifican algunos DI como la pornografía infantil, el acceso indebido a la información, sabotaje de sistemas informáticos, entre otros, que atentan contra el patrimonio de las personas (Mayer-Lux, 2018). Al respecto, en la tabla 1 se presentan las principales normas aplicadas en la región.

Tabla 1. ***Leyes de delitos informáticos en Latinoamérica***

PAÍS	NORMA	AÑO
Argentina	Ley 26.388	2008
Bolivia	Ley 1768	1997
Brasil	Lei 10.446	2002
	Lei 12.735	2012
	Lei 12.737	2012
Colombia	Ley 1273 de 2009	2009
Costa Rica	Ley 8148	2001
	Ley 9048	2012
Cuba	Decreto Ley 35	2021
	Ley 151	2022
Chile	Ley 21459	2022
Ecuador	Ley 30096	2013
El Salvador	Decreto 260	2016
Guatemala	Decreto 39	2022
Honduras	Decreto 130-2017	2019
México	Código Penal Federal	1931
Nicaragua	Ley 1042	2020
Panamá	Ley 14	2007
	Ley 51	2008
Paraguay	Ley 4439	2011
Perú	Ley 30096	2013
Puerto Rico	Ley 40	2024
	Ley 146	2012
	Ley 165	2008
República Dominicana	Ley 53	2007
Venezuela	Decreto 825	2000

Fuente: elaboración propia.

Resultados de investigación

1. Análisis descriptivo variables asociadas a delitos informáticos

A continuación se presentan los resultados descriptivos del comportamiento de las variables asociadas a los DI. En la tabla 2 se aprecian los resultados de la denuncia por país. Los resultados revelan que el mayor número de denuncias se realizaron en Argentina (47,10%), México (13,05%) y Colombia (9,42%). Mientras tanto, los países en los que menos se realizaron denuncias fueron

Cuba (0,19%), Haití (0,38%) y Puerto Rico (0,38%). El año 2017 se destacó por el mayor número de denuncias de los años analizados (2760), siendo Argentina el país que mayor número de denuncias recibió (41,34%), seguido de México (17,86%) y Colombia (11,23%).
Cabe destacar que en Argentina, México y Colombia se han venido haciendo grandes esfuerzos por combatir los delitos informáticos y los ciudadanos están más dispuestos a realizar la denuncia antes de dejar pasar el incidente por alto. A pesar de los esfuerzos que se hacen en la región, hay países que tienen indicadores muy bajos en las denuncias como sucede con Cuba, Haití y Puerto Rico, por lo que está en manos de los entes de seguridad ciudadana promover en la ciudadanía la denuncia de los delitos informáticos a fin de castigar a los delincuentes y controlar este problema.

Tabla 2. ***Denuncia por país***

Denuncia por país	**2015**		**2016**		**2017**		**Total**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Argentina	670	51,94	690	54,76	1141	41,34	2501	47,10
Bolivia	40	3,10	30	2,38	28	1,01	98	1,85
Brasil	70	5,43	10	0,79	28	1,01	108	2,03
Colombia	80	6,20	110	8,73	310	11,23	500	9,42
Costa Rica	10	0,78	10	0,79	29	1,05	49	0,92
Cuba	10	0,78	0	0,00	0	0,00	10	0,19
Chile	30	2,33	10	0,79	127	4,60	167	3,15
Ecuador	0	0,00	60	4,76	56	2,03	116	2,18
El Salvador	0	0,00	0	0,00	28	1,01	28	0,53
Guatemala	30	2,33	40	3,17	141	5,11	211	3,97
Haití	10	0,78	10	0,79	0	0,00	20	0,38
Honduras	30	2,33	100	7,94	56	2,03	186	3,50
México	140	10,85	60	4,76	493	17,86	693	13,05
Nicaragua	20	1,55	10	0,79	28	1,01	58	1,09
Panamá	30	2,33	10	0,79	14	0,51	54	1,02
Paraguay	10	0,78	0	0,00	14	0,51	24	0,45
Perú	40	3,10	30	2,38	169	6,12	239	4,50
Puerto Rico	10	0,78	10	0,79	0	0,00	20	0,38
República Dominicana	10	0,78	20	1,59	0	0,00	30	0,56
Uruguay	0	0,00	30	2,38	28	1,01	58	1,09
Venezuela	50	3,88	20	1,59	70	2,54	140	2,64
Total	1290	100,00	1260	100,00	2760	100,00	5310	100,00

Fuente: elaboración propia

En la tabla 3 se aprecian los resultados sobre el tipo de víctima, ocupando el primer lugar la persona física (84,23%) seguido de la PYME (9,58%). Asimismo, los resultados revelan que la persona física es la víctima con más presencia en el 2015 (72,22%), 2016 (84,00%) y 2017 (89,82%).
Queda en evidencia que los delitos informáticos en las grandes empresas y los organismos gubernamentales es poco recurrente, probablemente por los sistemas de ciberseguridad que tienen instalado en sus equipos.

Tabla 3. ***Tipo de víctima***

Tipo de victima	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
Persona física	910	72,22	1050	84,00	2479	89,82	4439	84,23
PYME	140	11,11	140	11,20	225	8,15	505	9,58
Empresa con más de 100 empleados	140	11,11	20	1,60	28	1,01	188	3,57
Organismos gubernamentales	70	5,56	40	3,20	28	1,01	138	2,62
Total	1260	100,00	1250	100,00	2760	100,00	5270	100,00

Fuente: elaboración propia

En cuanto a la edad de las víctimas por delitos informáticos el primer lugar lo ocupó el grupo entre 22 y 35 años (42,87%) y el segundo lugar entre 36 y 45 (23,11%), por lo tanto, son los grupos que más afectados (tabla 4).

Tabla 4. ***Edad***

Edad	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
Menos de 21	200	19,23	300	25,00	549	20,52	1049	21,34
Entre 22 y 35	470	45,19	440	36,67	1197	44,75	2107	42,87
Entre 36 y 45	210	20,19	250	20,83	676	25,27	1136	23,11
Más de 45	160	15,38	210	17,50	253	9,46	623	12,68
Total	1040	100,00	1200	100,00	2675	100,00	4915	100,00

Fuente: elaboración propia.

En la tabla 5 se aprecia la distribución del sexo en los años de estudio. Los resultados revelan que el 51,33% son de sexo femenino; mientras que el 48,67% son de sexo masculino. Al respecto se puede decir los porcentajes son muy cercanos, lo que deja en evidencia que el sexo es indiferente en los delitos informáticos.

Tabla 5. ***Sexo***

Sexo	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
Masculino	580	59,18	650	54,17	1113	42,26	2343	48,67
Femenino	400	40,82	550	45,83	1521	57,74	2471	51,33
Total	980	100,00	1200	100,00	2634	100,00	4814	100,00

Fuente: elaboración propia.

En la tabla 6 se aprecia el nivel de instrucción de los afectados por delitos informáticos. Los resultados muestran que las personas con nivel de instrucción universitaria (57,60%) y segundaria (30,03%) son los que tienen mayor participación. Lo expuesto, queda evidenciado en el comportamiento de las variables en los diferentes años, por ejemplo, como sucede con el nivel universitario en el 2015 (56,57%), 2016 (58,97%) y 2017 (57,37%).

Tabla 6. ***Nivel de instrucción***

Instrucción	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
Sin instrucción	50	5,05	40	3,42	99	3,84	189	3,99
Primaria	150	15,15	120	10,26	127	4,93	397	8,38
Segundaria	230	23,23	320	27,35	873	33,86	1423	30,03
Universitaria	560	56,57	690	58,97	1479	57,37	2729	57,60
Total	990	100,00	1170	100,00	2578	100,00	4738	100,00

Fuente: elaboración propia.

En la tabla 7 se revela información sobre la denuncia realizada. Cabe destacar que un 79,64% de las personas no ha denunciado por razones personales y los que denunciaron (11,17%) señalaron que la investigación no avanzó. Apenas el 0,73% de los delincuentes fue condenado. Lo expuesto, deja en evidencia que no existe la cultura de la denuncia y hay razones diversas que pueden estar vinculadas a ello.

Tabla 7. ***Ha denunciado***

Ha denunciado	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
No, no denuncié porque...	880	68,22	1040	82,54	2309	83,66	4229	79,64
Si, ya denuncié y la investigación está en curso	210	16,28	70	5,56	169	6,12	449	8,46
Si, denuncié pero la investigación no avanzó	200	15,50	140	11,11	253	9,17	593	11,17
Si, denuncié y ya se ha condenado al o los culpables	0	0,00	10	0,79	29	1,05	39	0,73
Total	1290	100,00	1260	100,00	2760	100,00	5310	100,00

Fuente: elaboración propia.

En la tabla 8 se muestran las causas por las que no se ha denunciado por el miedo a la pérdida de confidencialidad (15,44%), no cree en el éxito de la investigación (15,27%), no sabe dónde denunciar (14,44%, tiene temor a futuras represalias (13,58%) entre otras razones.

Tabla 8. ***Causas por las que no denunció***

Causas por las que no denunció	2015		2016		2017		Total	
	f	%	f	%	f	%	f	%
No creo que la investigación tenga éxito	219	16,98	204	16,19	388	14,06	811	15,27
No quiero difundir públicamente el incidente (perdida de confidencialidad)	219	16,98	156	12,38	445	16,12	820	15,44
No creo en la policía ni en la justicia penal	155	12,02	108	8,57	251	9,09	514	9,68
No creo que la denuncia sea útil, porque el sistema penal no está apto para combatir el cibercrimen	155	12,02	72	5,71	468	16,96	695	13,09
Tengo temor de futuras represalias de parte del autor	129	10,00	204	16,19	388	14,06	721	13,58
No sé dónde denunciar	116	8,99	240	19,05	411	14,89	767	14,44
No me tomaron la denuncia	90	6,98	60	4,76	57	2,07	207	3,90
En parte me siento culpable del incidente	90	6,98	12	,95	91	3,30	193	3,63
No me considero víctima de un delito	65	5,04	168	13,33	171	6,20	404	7,61
Otros	52	4,03	36	2,86	90	3,26	178	3,35

Total	1290	100,00	1260	100,00	2760	100,00	5310	100,00

Fuente: elaboración propia.

Los tipos de incidentes de delitos informáticos son diversos. En la tabla 9 se aprecia que los que tienen mayor incidencia son calumnias en injurias (16,06%), amenazas (14,81%) y Hacking (14,02%). En menor proporción pero no menos importante se encuentran denegación del servicio (2,42%), difusión de malware (3,84%) y pornografía infantil (4,16%).

En los últimos años los hacking han causado delitos innumerables debido a la implantación de virus que infectan los programas a fin de eliminarlos, recibiendo a cambios, cuantiosas sumas de dinero. La proliferación de los hacking ha llevado a las organizaciones a blindarse con peritos informáticos forenses de cara combatir esta problemática. Las organizaciones también están enfrentando problemas con el robo de proyectos, los cuales son plagiados y comercializados ilegalmente lo que genera impactos económicos negativos. El robo de información normalmente es difícil detectarlo por la diversidad de personas involucradas, que pueden ser colaboradores de la organización y personas externas. Este sabotaje organizacional, puede venir acompañado de calumnias e injurias que perjudican la reputación y el trabajo del equipo de colaboradores (Steinmetz, 2022).

Las calumnias e injurias es uno de los delitos informáticos que más se cometen a través de las redes sociales y, son acciones que atentan contra la dignidad de personas y busca desprestigiarla. Otro de los delitos comunes en Latinoamérica es el phishing que consiste en la suplantación de identidad a fin de obtener información sensible, delito muy común en el sector financiero; razón por la cual los bancos han diseñado diversas estrategias, por ejemplo los *tokens*, a fin de hacer transacciones más seguras. Cabe destacar que el grooming aumentó drásticamente del 2015 (50 afectados) al 2017 (141 afectados) lo que deja en evidencia el interés de los delincuentes para lograr obtener material sensible de las victimas a fin usar el chantaje como medio de extorción (Rincón-Arteaga, Castiblanco-Hernández, Quijano-Díaz, Urquijo-Vanegas & Pregonero-León, 2023).

Tabla 9. ***Incidente***

Incidente	**2015**		**2016**		**2017**		**Total**	
	f	**%**	**f**	**%**	**f**	**%**	**F**	**%**
Hacking	290	25,00	170	15,18	211	8,42	671	14,02
Calumnias e injurias	220	18,97	140	12,50	408	16,28	768	16,05
Amenazas	110	9,48	120	10,71	479	19,11	709	14,81
Fraude o estafa informática	110	9,48	160	14,29	338	13,49	608	12,70
Cracking	100	8,62	110	9,82	84	3,35	294	6,14
Phishing	100	8,62	120	10,71	296	11,81	516	10,78
Violación de datos personales	100	8,62	100	8,93	310	12,37	510	10,66
Grooming	50	4,31	20	1,79	141	5,63	211	4,41
Difusión de malware	40	3,45	60	5,36	84	3,35	184	3,84
Denegación de servicio	20	1,72	40	3,57	56	2,23	116	2,42
Pornografía infantil	20	1,72	80	7,14	99	3,95	199	4,16
Total	1160	100,00	1120	100,00	2506	100,00	4786	100,00

Fuente: elaboración propia.

en la tabla 10 se revela que el 71,41% de los afectados por delitos informáticos dejó correo electrónico; mientras que el 28,59% no lo hicieron.

Tabla 10. ***Correo electrónico***

Correo electrónico	2015		2016		2017		Total	
	f	%	f	%	f	%	F	%
Dejaron correo electrónico	810	62,79	870	69,05	2112	76,52	3792	71,41
No dejaron correo electrónico	480	37,21	390	30,95	648	23,48	1518	28,59
Total	1290	100,00	1260	100,00	2760	100,00	5310	100,00

Fuente: elaboración propia.

2. Relación entre variables asociadas a los delitos informáticos

De la relación de la denuncia por país y el sexo de deriva que el sexo masculino tiene su presencia total en Argentina. Mientras que, la distribución del sexo femenino tiene mayor presencia en México (22,38%), Colombia (20,23%) y Guatemala (8,54%). En este sentido, a pesar que la cantidad de hombre y mujeres es cercana, se nota que las mujeres en Latinoamérica están perdiendo el miedo a denunciar y hacer valer sus derechos (tabla 11).

Tabla 11. ***Relación sexo y denuncia por país***

Denuncia por país	Sexo					
	Masculino		Femenino		Total	
	f	%	f	%	f	%
Argentina	2343	100,00	158	6,39	2501	51,95
Bolivia	0	0,00	98	3,97	98	2,04
Brasil	0	0,00	108	4,37	108	2,24
Colombia	0	0,00	500	20,23	500	10,39
Costa Rica	0	0,00	49	1,98	49	1,02
Cuba	0	0,00	10	0,40	10	0,21
Chile	0	0,00	167	6,76	167	3,47
Ecuador	0	0,00	116	4,69	116	2,41
El Salvador	0	0,00	28	1,13	28	0,58
Guatemala	0	0,00	211	8,54	211	4,38
Haití	0	0,00	20	0,81	20	0,42
Honduras	0	0,00	186	7,53	186	3,86
México	0	0,00	553	22,38	553	11,49
Nicaragua	0	0,00	38	1,54	38	0,79
Panamá	0	0,00	24	0,97	24	0,50
Paraguay	0	0,00	14	,57	14	0,29
Perú	0	0,00	171	6,92	171	3,55
Puerto Rico	0	0,00	10	0,40	10	0,21
República Dominicana	0	0,00	10	0,40	10	0,21
Total	2343	100,00	2471	100,00	4814	100,00

Fuente: elaboración propia.

En la tabla 12 se aprecia la relación del nivel de instrucción y si ha denunciado. Los resultados revelan que un alto porcentaje de los que no han denunciado tienen nivel universitario (81,35%).

Cabe destacar que este comportamiento se sigue presentando en las variables relacionadas con "si, ya denuncié y la investigación está en curso" (12,79%) y "si, denuncié pero la investigación no avanzó" (5,86%).

Tabla 12. ***Relación entre nivel de instrucción y ha denunciado***

Ha denunciado	Sin instrucción		Primaria		Segundaria		Universitaria		Total	
	f	%	f	%	f	%	f	%	f	%
No, no denuncié porque...	189	100,00	397	100,00	1423	100,00	2220	81,35	4229	89,26
Si, ya denuncié y la investigación está en curso	0	0,00	0	0,00	0	0,00	349	12,79	349	7,37
Si, denuncié pero la investigación no avanzó	0	0,00	0	0,00	0	0,00	160	5,86	160	3,38
Total	189	100,00	397	100,00	1423	100,00	2729	100,00	4738	100,00

Fuente: elaboración propia.

En cuanto a la relación entre el incidente y el tipo de víctima se encuentra que las personas físicas son las que más denuncian los delitos informáticos, sobre todo, en delitos como calumnias e injurias (17,30%), amenazas (15,97%) y hacking (15,12%) (tabla 13).

Tabla 13. ***Relación entre tipo de víctima e incidente***

Incidente	Persona física		PYME		Empresa con más de 100 empleados		Total	
	f	%	f	%	f	%	f	%
Hacking	671	15,12	0	0,00	0	0,00	671	14,02
Calumnias e injurias	768	17,30	0	0,00	0	0,00	768	16,05
Amenazas	709	15,97	0	0,00	0	0,00	709	14,81
Fraude o estafa informática	608	13,70	0	0,00	0	0,00	608	12,70
Cracking	294	6,62	0	0,00	0	0,00	294	6,14
Phishing	496	11,17	20	8,44	0	0,00	516	10,78
Violación de datos personales	410	9,24	100	42,19	0	0,00	510	10,66
Grooming	161	3,63	20	8,44	30	27,27	211	4,41
Difusión de malware	144	3,24	0	0,00	40	36,36	184	3,84
Denegación de servicio	96	2,16	0	0,00	20	18,18	116	2,42
Pornografía infantil	82	1,85	97	40,93	20	18,18	199	4,16
Total	4439	100,00	237	100,00	110	100,00	4786	100,00

Fuente: elaboración propia.

En la tabla 14 se aprecia la relación entre las causas por las cuales no denunció y la edad. Las personas con edad entre 22 y 35 son las que más participación tienen del grupo de estudio. Al respecto, las causas por las que no denunciaron están relacionadas con las variables "no creo que la denuncia sea útil, porque el sistema penal no está apto para combatir el cibercrimen" (29,28%), "no quiero difundir públicamente el incidente (perdida de confidencialidad)" (26,72%) y "no creo en la policía ni en la justicia penal" (24,39%).

Tabla 14. ***Relación entre causas por las que no denunció y edad***

Causas por las que no denunció	Menos de 21		Entre 22 y 35		Entre 36 y 45		Más de 45		Total	
	f	%	f	%	f	%	f	%	F	%
No creo que la investigación tenga éxito	792	75,50	19	0,90	0	0,00	0	0,00	811	16,50
No quiero difundir públicamente el incidente (perdida de confidencialidad)	257	24,50	563	26,72	0	0,00	0	0,00	820	16,68
No creo en la policía ni en la justicia penal	0	0,00	514	24,39	0	0,00	0	0,00	514	10,46
No creo que la denuncia sea útil, porque el sistema penal no está apto para combatir el cibercrimen	0	0,00	617	29,28	78	6,87	0	0,00	695	14,14
Tengo temor de futuras represalias de parte del autor	0	0,00	394	18,70	327	28,79	0	0,00	721	14,67
No sé dónde denunciar	0	0,00	0	0,00	654	57,57	113	18,14	767	15,61
No me tomaron la denuncia	0	0,00	0	0,00	63	5,55	101	16,21	164	3,34
En parte me siento culpable del incidente	0	0,00	0	0,00	14	1,23	89	14,29	103	2,10
No me considero víctima de un delito	0	0,00	0	0,00	0	0,00	315	50,56	315	6,41
Otros	0	0,00	0	0,00	0	0,00	5	0,80	5	0,10
Total	1049	100,00	2107	100,00	1136	100,00	623	100,00	4915	100,00

Fuente: elaboración propia.

Conclusiones

Los DI atentan contra la privacidad de las personas y organizaciones. Los ciberdelincuentes han encontrado un espacio para el enriquecimiento ilícito, el robo de información y desestabilización de la integridad de los afectados. A fin de combatir los DI las organizaciones están recurriendo a la auditoría a fin de lograr obtener pruebas ante procesos judiciales. La auditoría permite la detección del DI y la creación de dispositivos que protejan a las organizaciones de injerencias de extraños que atenten contra el capital y la reputación. De ahí que una de las estrategias para protegerse de los DI es la auditoría de sistemas a fin de detectar cualquier violación o irregularidad del sistema de seguridad.

Hoy día todavía existen vacíos legales en Latinoamérica en cuanto a los DI que deben ser corregidos de cara a combatir los actos ilícitos y sancionar a los infractores. No basta con la existencia de un cuerpo de normas que regulen los delitos si el aparato judicial es inoperante y no da solución inmediata a las acciones delictivas. Con el desarrollo tecnológico se incrementa el DI, por ello, los funcionarios judiciales deben estar preparados para dar respuesta a los atentados informáticos y el uso indebido de las TIC.

No basta con tener una estructura jurídica idónea sobre los DI, también hace falta que los entes investigadores cuenten con la formación y los equipos necesarios para llevar a cabo su trabajo. Asimismo, la cooperación internacional es necesaria a fin de desplegar dispositivos de seguridad para castigar a los delincuentes por los delitos cometidos en el extranjero.

Referencias

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana De Gerencia*, 25(89), 351-368. https://doi.org/10.37960/revista.v25i89.31534

Alcívar-Trejo, C., Blanc-Pihuave, G., & Calderón-Cisneros, J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. Espacios, 39(42), 15-24. https://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Arcos-Argudo, M., Matute-Pinos, K., & Fernández-Mora, M. (2023). Comparative analysis of the Organic Law on Personal Data Protection of Ecuador with Colombian legislation from a cybersecurity and cybercrime approach. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, E60, 100 – 114. https://www-scopus-com.sibulgem.unilibre.edu.co/record/display.uri?eid=2-s2.0-85169424188&origin=resultslist&sort=plf-f&src=s&sid=62c76d05507bb152eb930b409f5e61d1&sot=b&sdt=b&s=TITLE%28delitos+informaticos%29&sl=27&sessionSearchId=62c76d05507bb152eb930b409f5e61d1&relpos=2

Blázquez-Agudo, E. M. (2021). Gestión y aplicación empresarial de las exigencias sobre protección de datos personales. *Revista del Ministerio de Trabajo y Economía Social*, 148, 399-429. https://dialnet.unirioja.es/servlet/articulo?codigo=8090223

Código Penal federal. (14 de agosto de 1931). Código Penal Federal. https://mexico.justia.com/federales/codigos/codigo-penal-federal/gdoc/

Consejo Europeo. (2001). Convenio de la ciberdelincuencia. Budapest: Consejo Europeo. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo Europeo. (2008). Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. https://rm.coe.int/1680a7bbf3

Debortoli, D. O., & Brignole, N. B. (2024). Inteligencia empresarial para estimular el giro comercial en el microcentro de una ciudad de tamaño intermedio. *Región Científica*, 3(1), 2024195. https://doi.org/10.58763/rc2024195

Decreto 825. (10 de mayo de 2000). Decreto Mediante el cual se Declara el Acceso y el Uso de Internet como Política Prioritaria para el Desarrollo Cultural, Económico, Social y Político de la República Bolivariana de Venezuela. https://docs.venezuela.justia.com/federales/decretos/decreto-n-825.pdf

Decreto Ley 35. (17 de agosto de 2021). De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del Espectro Radioeléctrico. https://www.minjus.gob.cu/sites/default/files/archivos/publicacion/2021-08/goc-2021-o92.pdf

Decreto 260. (26 de febrero de 2016). Ley Especial contra los Delitos Informáticos y Conexos. https://www.fiscalia.gob.sv/medios/portal-transparencia/normativas/normativas-de-interes/ley-especial-contra-delitos-ciberneticos.pdf

Decreto 39. (24 de agosto de 2022). Ley de Prevención y Protección contra la Ciberdelincuencia. https://www.soy502.com/sites/default/files/decreto-39-2022.pdf

Decreto 130-2017. (31 de enero de 2019). Código Penal. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

de-la-Garza-Montemayor, D. J., & Leal-Espinoza, J. L. (2020). Derecho a la información y protección de datos personales en el neoconstitucionalismo iberoamericano: Abordaje principialista de la tutela efectiva desde la teoría de los derechos humanos. *Nuevo Derecho*, 16(27), 1-14. https://doi.org/10.25057/2500672X.1358

Eslava-Zapata, R., Ferney-Archila, A., Mogrovejo-Andrade, J. M., Chacón-Guerrero, E., & Esteban-Montilla, R. (2024). Planeación estratégica en empresas comercializadoras de textiles. *Universidad Y Sociedad*, 16(1), 550-560. https://rus.ucf.edu.cu/index.php/rus/article/view/4358

Eslava-Zapata, R,, Omaña-Guerrero, J. A., Sierra-Narváez, F. J., & Mogrovejo-Andrade, J. M. (2023). Estilos de liderazgo: un estudio en Latinoamérica, Estados Unidos y Europa. *Salud, Ciencia y Tecnología*, 3, 1-8. https://doi.org/10.56294/saludcyt2023401

Fakiha, B. (2023). The Role of Raspberry Pi in Forensic Computer Crimes. *Journal of Internet Services and Information Security*, 13(4), 76–87. https://doi.org/10.58346/JISIS.2023.I4.005

Fernández, W., & Vargas, C. (2018). ¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías. *Law, State and Telecommunications Review*, 10(2), 37–52. https://doi.org/10.26512/lstr.v10i2.21492

Gascón-Marcén, A. (2021). The general data protection regulation as a model of recent european digital draft legislation. *Cuadernos de Derecho Transnacional*, 13(2), 209 – 232. https://doi.org/10.20318/cdt.2021.6256

Guatemala-Mariano, A., & Martínez-Prats, G. (2023). Capacidades tecnológicas en empresas sociales emergentes: una ruta de impacto social. *Región Científica*, 2(2), 2023111. https://doi.org/10.58763/rc2023111

Guerrero-Guerrero, B. (2020). Protección de datos personales en el Poder Judicial: Una nueva mirada al principio de publicidad de las actuaciones judiciales. *Revista Chilena De Derecho Y Tecnología*, 9(2), 33–56. https://doi.org/10.5354/0719-2584.2020.54372

Graves, J. T., & Acquisti, A. (2023). An empirical analysis of sentencing of "Access to Information" computer crimes. *Journal of Empirical Legal Studies*, 20(2), 434–471. https://doi-org.sibulgem.unilibre.edu.co/10.1111/jels.12349

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. d. P. (2014). *Metodología de la investigación*. Sexta edición. México: McGraw Hill.

Iancu, E. A., Tușa, E., Iancu, N., Simion, E., & Moise, A. C. (2023). Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems. *Juridical Tribune*, 13(3), 365–383. https://doi.org/10.24818/TBJ/2023/13/3.03

Lei 10.446. (8 de maio de 2002). Dispõe sobre infrações penais de repercução interestadual o internacional que exigem repressão uniforme, para os fins do disposto no inciso I del § 1o do art. 144 da Constituição. http://www.planalto.gov.br/ccivil_03/leis/2002/L10446.htm

Lei 12.735. (30 de novembro de 2012). Portal da Legislação. http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm

Lei 12.737. (30 de novembro de 2012). Portal da Legislação. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Ley 1273. (5 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ley 8148 (24 de octubre de 2001). Adición de los Artículos 196 Bis, 217 Bis y 229 Bis al Código Penal Ley Nº 4573, para reprimir y sancionar los delitos informáticos. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47430&nValor3=50318&strTipM=TC#:~:text=Ser%C3%A1%20reprimida%20con%20pena%20de,datos%20e%20im%C3%A1genes%20contenidas%20en

Ley 9048. (10 de julio de 2012). Reforma de varios Artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

Ley 4439. (2011). Que modifica y amplia varios Articulos de la Ley n° 1160/97 “Codigo Penal” el Congreso de la Nación paraguaya sanciona con fuerza de Ley. https://www.bacn.gov.py/archivos/3777/20150817113434.pdf

Ley 30096. (23 de octubre de 2013). Ley de Delitos Informáticos. https://cdn.www.gob.pe/uploads/document/file/1671764/1678028-ley-n-30096-ley-de-delitos-informaticos-vigente-pdf.pdf?v=1708709859

Ley 26.388. (25 de junio de 2008). Delitos Informáticos y Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley 1768. (10 de marzo de 1997). Ley de modificaciones al Código Penal. Delitos de propiedad intelectual y delitos informáticos. https://derechodelacultura.org/wp-content/uploads/2015/03/Bolivia-Codigo-Penal-1997.pdf?view=download

Ley 151. (01 de septiembre de 2022). Código Penal. https://www.parlamentocubano.gob.cu/sites/default/files/documento/2022-09/goc-2022-o93_0.pdf

Ley 21459 (20 de junio de 2022). Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. https://www.bcn.cl/leychile/navegar?idNorma=1177743

Ley 1042. (27 de octubre de 2020). Ley Especial de Ciberdelitos. http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87

Ley 14. (18 de mayo de 2007). Texto Único del Código Penal de la República de Panamá. https://ministeriopublico.gob.pa/wp-content/uploads/2016/09/codigo-penal-2016.pdf

Ley 51. (21 de junio de 2008). Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. https://www.gacetaoficial.gob.pa/pdfTemp/26090/GacetaNo_26090_20080724.pdf

Ley 30096. (27 de septiembre de 2013). Ley de Delitos Informáticos. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Ley 40. (18 de enero de 2024). Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico. https://www.lexjuris.com/lexlex/Leyes2024/lexl2024040.htm

Ley 165. (06 de agosto de 2008). Ley de Regulación de Programación de Espionaje Cibernético. https://bvirtualogp.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Informatica/165-2008.pdf

Ley 146. (30 de julio de 2012). Código Penal de Puerto Rico. https://bvirtualogp.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Justicia/146-2012/146-2012.pdf

Ley 53. (17 de enro de 2007). Sobre Crímenes y Delitos de Alta Tecnología. https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

Linares, M. B. (2020). Delitos informáticos en el Código penal argentino. *Revista Chilena de Derecho y Ciencia Política*, 11(2), 122-144. https://doi.org/10.7770/rchdcp-V11N2-art2289

Mattace, G. (2024). The protection of children's personal data in the digital space. *Actualidad Juridica Iberoamericana*, 20, 1418-1439. https://dialnet.unirioja.es/servlet/articulo?codigo=9311296

Mayer-Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, 24(1), 159-206. http://dx.doi.org/10.4067/S0718-00122018000100159

Mejía-Lobo, M., Hurtado-Gil, S. V., & Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista De Ciencias Sociales*, 29(2), 356-372. https://doi.org/10.31876/rcs.v29i2.39981

Navarro-Dolmestch, R. (2023). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos. *Revista Chilena De Derecho Y Tecnología*, 12, 1–24. https://doi.org/10.5354/0719-2584.2023.67546

Observatorio de Delitos Informáticos de Latinoamérica (2015). *Informe 2015*. Argentina: ODILA. Obtenido https://www.odila.org/reporte-2015

Observatorio de Delitos Informáticos de Latinoamérica (2016). *Informe 2016*. Argentina: ODILA. Obtenido de https://www.odila.org/reporte-2016

Observatorio de Delitos Informáticos de Latinoamérica (2017). *Informe 2017*. Argentina: ODILA. Obtenido de https://www.odila.org/reporte

Rincón-Arteaga, J. A., Castiblanco-Hernández, S. A., Quijano-Díaz, A., Urquijo-Vanegas, J. D., & Pregonero-León, Y. K. (2023). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad*, 64(3), 95–116. https://doi.org/10.47741/17943108.368

Rodríguez-Ayuso, J. F. (2021). Estado de alarma y protección de la privacidad en tiempos de pandemia. *Revista de Derecho Político*, 110, 299-318. https://dialnet.unirioja.es/servlet/articulo?codigo=7824428

Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). The protection of personal data in Ecuador: A historical-normative review of this fundamental right in the South American country. *Revista Internacional De Cultura Visual*, 13(2), 1-16. https://doi.org/10.37467/revvisual.v10.4568

Sánchez-Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana De Derecho Administrativo*, 10(1), e235. https://doi.org/10.14409/redoeda.v10i1.12626

Santacruz, H. B., & Hermoza, M. M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação*, E20, 391-400. https://www.proquest.com/openview/fc081b269b3464d67367cafb7a4b1d66/1?pq-origsite=gscholar&cbl=1006393

Santana-Martínez, J. A., Romero-Zapata, A. S., & Camacho-Bobadilla, C. E. (2023). Análisis de la relevancia de la identidad visual y branding en las ideas de negocio. *Revista Gestión y Desarrollo Libre*, 8(16), 1-15. https://doi.org/10.18041/2539-3669/gestionlibre.16.2023.10224

Steinmetz, K. F. (2022). Crime in the Age of the Smart Machine: A Zuboffian Approach to Computers and Crime. *International Journal for Crime, Justice and Social Democracy*, 11(1), 225-238. https://doi.org/10.5204/ijcjsd.2136.

Subanjui, R., Wattanakomol, S., & Silpcharu, T. (2023). Guidelines on the Prevention of Offenses under Thailand's Computer-Related Crime Act for Industrial Business. *WSEAS Transactions on Business and Economics*, 20, 931–940. https://doi.org/10.37394/23207.2023.20.86

Šupa, M., Kaktinas, V., & Rinkevičiūtė, A. (2023). Computer-dependent or computer-assisted? The social context of online crime in Lithuanian court judgements. *International Journal of Law, Crime and Justice*, 73, 100577. https://doi.org/10.1016/j.ijlcj.2023.100577

Stratonov, V., Slinko, D., & Slinko, S. (2021). Some Types of Computer Crime and Cybercrime in Ukraine. *Access to Justice in Eastern Europe*, 3(11), 191–197. https://doi.org/10.33327/AJEE-18-4.3-n000078

Tamayo-Medina, A. I., Carvajal-Guerrero, A. M., & Maldonado-Niño, L. G. (2023). E-commerce como herramienta para el desarrollo regional y competitivo de los sectores productivos: estudio empírico. *Revista Gestión y Desarrollo Libre*, 8(15), 1-16.https://doi.org/10.18041/2539-3669/gestionlibre.15.2023.10104

Vázquez-Cano, E., & Pascual -Moscoso, C. (2022). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, 25(3), 95–110. https://doi.org/10.6018/reifop.529831

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2019). Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação*, E17, 671-677. https://www.proquest.com/openview/b7f8919dbb75fa3e5f21552a48e94816/1?pq-origsite=gscholar&cbl=1006393