Imagen que contiene Diagrama

Descripción generada automáticamente**UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO**

**FACULTAD DE CIENCIAS PARA LA INGENIERÍA**

**CARRERA: INGENIERÍA EN SOFTWARE**

**INTEGRANTES:**

Aviles Chalaco Diana Stefania

Zambrano Monserrate Dennisse Paola

**DOCENTE:**

Ing. Guerrero Ulloa Gleiston Ciceron

**TEMA:**

Legislación Informática en Ecuador

**MATERIA:**

Legislación Informaática

**CURSO:**

10mo Semestre “A”

**AÑO LECTIVO:**

2023- 2024

**QUEVEDO – LOS RÍOS – ECUADOR**

**Índice**

[Introducción 3](#_Toc153660885)

[Desarrollo 3](#_Toc153660886)

[El derecho y los derechos 3](#_Toc153660887)

[Impacto de los delitos informáticos 5](#_Toc153660888)

[Estadísticas sobre delitos 6](#_Toc153660889)

[Protección de datos de nivel personal 8](#_Toc153660890)

[Sujetos procesales 9](#_Toc153660891)

[Conclusión 10](#_Toc153660892)

[Referencia 11](#_Toc153660893)

**Enlace a repositorio**

<https://github.com/DianaAvilesCh/Legislacion_GrupoTA>

# **Introducción**

La legislación informática en Ecuador es un tema importante que aborda varios aspectos relacionados con el uso de la tecnología. En este resumen se presentan los temas más relevantes sobre la legislación informática en Ecuador. El derecho informático es una rama del derecho que se encarga de regular el uso de la tecnología de la información y la comunicación. En Ecuador, el derecho informático se encuentra regulado por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos [1]. Esta ley establece los derechos y obligaciones de las partes que intervienen en una transacción electrónica.

# **Desarrollo**

## **El derecho y los derechos**

El concepto de derecho es esencialmente complejo y ha sido objeto de debate entre juristas a lo largo del tiempo. La falta de consenso en torno a una definición precisa revela la amplitud y diversidad de este término, llevando a distintos autores a proponer enfoques variados. Desde la perspectiva de Kant, el derecho se vincula a la necesidad de acción por respeto a la ley, donde la ley se entiende como una norma que impone obligaciones. Leon Petrasizky y Giorgio del Vecchio contribuyen con sus distinciones entre normas impero-atributivas del derecho y normas morales, resaltando las diferencias estructurales y de finalidad entre ambas [1].

La coincidencia entre estas perspectivas radica en la conceptualización del derecho como un conjunto de normas. La dicotomía entre normas morales y jurídicas propuesta por Del Vecchio sugiere que toda regla de conducta pertenece a una de estas categorías. En este contexto, se adopta la noción de que el derecho, en su sentido jurídico, abarca un conjunto de leyes, normas, principios y reglas. Este conjunto regula la conducta de los miembros de una sociedad, estableciendo las bases para la convivencia bajo principios fundamentales de justicia, equidad y paz [1].

**El delito informático**

El delito informático, caracterizado por el uso de medios informáticos para violar bienes jurídicos protegidos, se ha convertido en una preocupación creciente en la sociedad ecuatoriana. Desde la perspectiva de Terragni, se define como una acción que causa perjuicio a personas, ya sea beneficiando al autor o no, y que está tipificada por la ley, sancionada con una pena. Esta definición destaca la importancia de considerar el daño causado más allá de la obtención de beneficios directos [2].

Julio Tellez introduce la noción de delitos informáticos como "crímenes de cuello blanco" cometidos por individuos con conocimientos en informática, enfocándose en la acción de un grupo selecto de técnicos. La obra también señala que estos delitos, perpetrados por personas con un coeficiente intelectual elevado y sin motivaciones económicas, buscan causar daño por placer, un aspecto novedoso que destaca la complejidad psicológica de estos actos [2].

El aumento de los delitos informáticos, facilitado por la accesibilidad a asesoramiento gratuito en línea, subraya la necesidad de incorporar sanciones más drásticas en la normativa legal ecuatoriana. La afirmación de que estos delitos son difíciles de probar resalta la importancia de contar con personal especializado en seguridad informática y de actualizar la normativa jurídica para abordar los nuevos desafíos y delitos que aún no están tipificados. En conclusión, la evolución de las telecomunicaciones y la creciente dependencia de medios informáticos exigen una legislación más rigurosa y actualizada para proteger la información y sancionar adecuadamente los delitos informáticos en Ecuador [2], [3].

**Clasificación de los delitos informáticos:**

* **Fraudes realizados a través de computadoras:** Estos delitos son frecuentes en los interiores de las Instituciones crediticias o bancarias, pues, las personas tienen facilidad de acceso a las bases de datos y registros de los usuarios.
* **Programación informática reproducida sin autorización:** Se trata de múltiples copias que se obtienen de programas que cuentan con licencia de uso, en nuestro medio, es comúnmente conocida como la piratería.
* **Manipulación de programas:** Esta modalidad se da a través de programas sustitutos que consienten y permiten manejar otros programas de mayor jerarquía y que cuentan con las licencias legales de cualquier organización o departamento estatal.
* **La manipulación de datos salientes:** Esta acción está destinada a adulterar los datos que son emitidos de una operación de cómputo, se realiza a través de otras computadoras.
* **Fraude por manipulación de la información:** Las personas que se dedican a esta modalidad, acceden a los programas que están en una base de datos informática, los manipulan con la finalidad de obtener una ganancia monetaria.
* **Falsificación informática:** Se da cuando una persona o grupos de personas, cambian la información que es emitida por una operación de consulta; es decir, manipulan los datos salientes de una base de datos.
* **Sabotaje informático:** Se trata de una interrupción de suministro de electrónica, telefonía e internet de manera intencional, para causar daño a los programas de cómputo.
* **Virus:** Se trata de la forma más peculiar de causar daño a los sistemas operativos, pues, son programas informáticos que se transfieren a las computadoras o equipos electrónicos y causan daño al perfecto funcionamiento de estos.

## **Impacto de los delitos informáticos**

Los ciberataques no solo representan una amenaza a la seguridad digital, sino que también generan un impacto negativo significativo en la situación económica de un país. La defensa contra los delitos informáticos se ha convertido en una lucha constante para personas y organizaciones, ya que los ciberdelincuentes están utilizando técnicas cada vez más complejas. Este aumento en la sofisticación de los ataques, como señalan Ponce Larreategui y Holguín Mendoza [4], [5], destaca la necesidad urgente de fortalecer las medidas de seguridad y prepararse para hacer frente a amenazas cada vez más avanzadas.

El crecimiento exponencial de los delitos informáticos se atribuye a diversos factores, como mencionan Batra et al. y Chévez Morán [6], [7]. Esta realidad subraya la importancia de profundizar en el análisis de casos específicos de este tipo de crímenes y estar debidamente preparados. Empresas individuales, comerciales y gubernamentales enfrentan amenazas constantes, lo que implica la necesidad de mantener una seguridad robusta en los sistemas empresariales. Los diseñadores de seguridad han introducido diversos perímetros de defensa, como firewalls y sistemas de detección y respuesta de amenazas, como parte de los esfuerzos para contrarrestar estas amenazas [8], [9].

La falta de conocimiento detallado sobre los delitos informáticos genera temor entre las personas, y esta aprehensión refuerza la necesidad de investigación para clasificar y comprender estos delitos. En este contexto, la investigación no solo es esencial para la identificación de patrones y técnicas utilizadas por los ciberdelincuentes, sino también para educar a la sociedad y fortalecer la conciencia sobre la importancia de la ciberseguridad. En conclusión, el impacto de los delitos informáticos es multidimensional y requiere una respuesta integral que incluya medidas de seguridad avanzadas, investigación continua y concientización pública.

## **Estadísticas sobre delitos**

En la siguiente tabla se traza la evolución histórica de los delitos cibernéticos desde los años 50 hasta la actualidad. Comenzando con el "phreaking" telefónico en los años 50, donde se aprovechaban fallas en sistemas telefónicos para realizar llamadas gratuitas, se pasó a la emergencia de términos como vulnerabilidades y piratería informática en los 60. El proyecto ARPANET en los 70 marcó el inicio de la ciberseguridad, siendo el lugar donde se creó el primer virus. En décadas posteriores, se experimentaron numerosos ataques informáticos, se establecieron pautas de seguridad y surgieron casos notables de ransomware en los 2010. Hoy en día, los ciberdelincuentes realizan ataques sofisticados respaldados por grandes corporaciones, ofreciendo servicios de delitos cibernéticos en plataformas digitales, y enfocándose cada vez más en entornos de redes sociales [10].

Tabla 1. Delitos cibernéticos.

|  |  |
| --- | --- |
| **Periodo - Décadas** | **Delitos cibernéticos** |
| 1950 | Comienza el phreaking telefónico |
| 1960 | Surgieron los términos de vulnerabilidad y piratería |
| 1970 | Apareció el término de seguridad informática. |
| 1980 | De ARPANET a Internet |
| 1990 | Los virus y gusanos informáticos se hicieron populares. |
| 2000 | El uso de Internet crece excesivamente |
| 2010 | Los ciberdelincuentes aprovecharon varias violaciones de seguridad y los delitos cibernéticos se convirtieron en una industria. |
| 2020 | Aumento del ciberdelito relacionado con las redes sociales |

El delito cibernético implica el uso de dispositivos electrónicos y acceso a Internet para cometer crímenes contra individuos u organizaciones. Las tasas de victimización por estos delitos, como robo de identidad, fraude con tarjetas de crédito, phishing y acceso no autorizado a cuentas, están en aumento. Se observa que en países menos desarrollados las tasas de victimización son más altas, señalando la necesidad de intervenciones preventivas en esas naciones [10]. La agenda global de ciberseguridad propone siete objetivos estratégicos para combatir estos delitos, que incluyen aspectos institucionales, técnicos, legales, cooperación internacional, aplicación de la ley, desarrollo de capacidades, concientización pública y alianzas público-privadas [11]

El informe sobre ciberseguridad en América Latina y el Caribe muestra un fuerte aumento en ciberataques a entidades públicas y privadas, así como a sitios web, creciendo más del 61% anualmente desde 2012. Países como Ecuador, Guatemala, Bolivia, Perú y Brasil están entre los más afectados por el malware. Uruguay, Colombia y Chile tienen tasas de infección de malware por encima del promedio global. En los últimos siete años, el uso del ciberespacio para cometer fraudes bancarios ha sido preocupante, con aproximadamente el 92% de las entidades financieras experimentando ciberataques, logrando un éxito del 37% [12]

Aunque la región latinoamericana está compuesta por numerosos países, la información disponible sobre ciberataques se centra en unos pocos países, tal como se describe en la siguiente figura. Los informes oficiales sobre ciberataques en América Latina se han enfocado en países como Panamá, Chile, Colombia, Ecuador, Argentina, Uruguay, Perú, Brasil y México. Sin embargo, estos datos solo muestran la cantidad de ataques sin considerar su impacto socioeconómico ni las consecuencias que puedan tener en las organizaciones y los países [12].

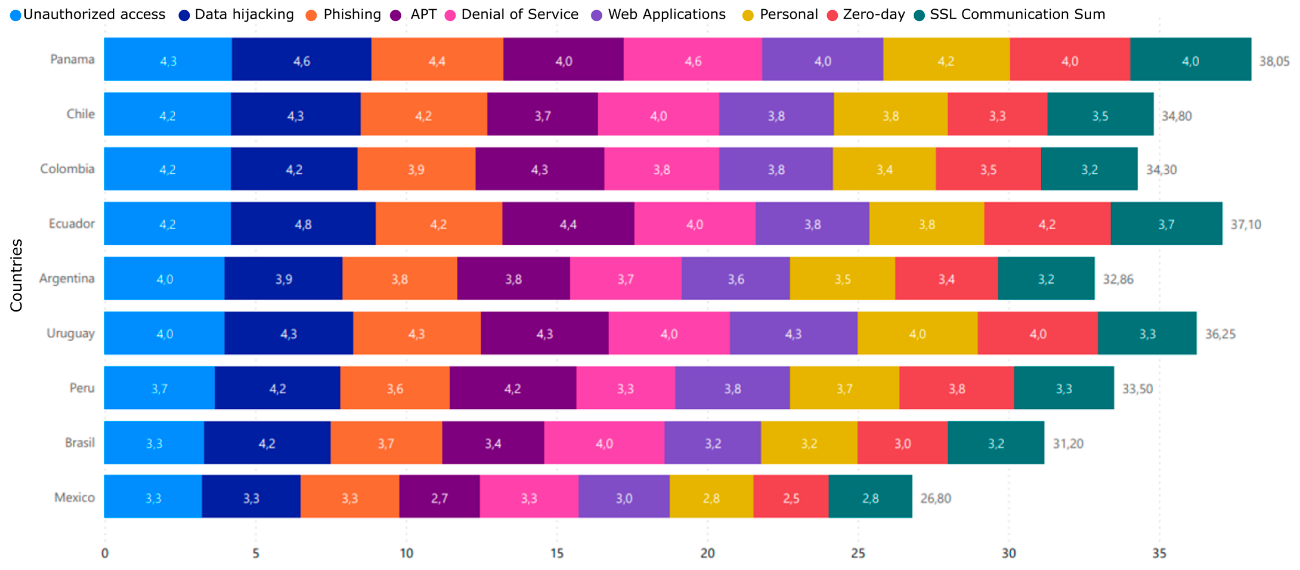


Figura . Niveles de efectos de los ciberataques en países de América Latina según el tipo de amenaza [12].

Ecuador enfrenta desafíos en la lucha contra el cibercrimen debido a una alta incidencia de incidentes registrados, mientras que su estrategia, Ecuador Digital, busca convertir al país en una sociedad de información y conocimiento a través de pilares como conectividad, eficiencia, ciberseguridad, innovación y competitividad. En comparación, países desarrollados como España tienen organizaciones públicas con mejores capacidades en ciberseguridad (más del 60% CMC), destacando la importancia del respaldo gubernamental y la colaboración internacional para fortalecer la ciberseguridad a nivel nacional [13].

El aumento de actividades delictivas informáticas es una tendencia global que también afecta a América Latina. En Ecuador, desde 2009 se ha observado un crecimiento en la discusión sobre los delitos informáticos, con un registro de 3,143 casos hasta 2013. Sin embargo, se estima que el 80% de estos delitos no son denunciados, lo que afecta el índice delictivo reportado. En comparación con otros países, Ecuador se sitúa en el tercer lugar en América Latina en este aspecto, con un 92% después de México (92%) y Bolivia (85%), según la ONU. Esta situación se atribuye a la falta de una cultura de denuncia. Según un artículo publicado en el diario El Comercio el 30 de enero de 2015, Ecuador ocupó el octavo lugar en la región en cuanto a la cantidad de ataques informáticos registrados en 2014, con un 28%, mientras que Brasil y Perú encabezaron la lista con un 32% y 28%, respectivamente [14].

## **Protección de datos de nivel personal**

Varios servicios en línea gratuitos, como buscadores y plataformas de redes sociales, emplean modelos comerciales que se apoyan en la recolección y tratamiento de información personal de sus usuarios. Esta información se analiza, alquila o vende con el fin de obtener ganancias. En esencia, los usuarios no abonan por los servicios mediante tarifas de suscripción u otro tipo de pago económico, sino más bien con sus datos personales [15].

Ecuador sigue siendo un país en proceso de desarrollo a través de las TIC, confía en los sistemas de información para sus diversos procedimientos. Esta dependencia crea una vulnerabilidad considerable frente a posibles ataques. A pesar de esto, Ecuador carece de una estrategia de política de seguridad, lo que hace necesario el apoyo e intervención de otras naciones para abordar esta situación [16].

A pesar de la ausencia de un plan estratégico en Ecuador, se implementan las siguientes acciones para mitigar los ciberataques dirigidos a instituciones tanto públicas como privadas [16]:

* Implementación de procesos de seguimiento del tráfico.
* Actualizar las credenciales de acceso es estrictamente complejo.
* Actualice todas las aplicaciones, especialmente como protección antivirus, para evitar la infiltración de elementos externos.
* Información de realización de los respaldos correspondientes.

## **Sujetos procesales**

Los sujetos procesales en la legislación informática son las personas que intervienen en un proceso judicial relacionado con la informática. Estos sujetos pueden ser partes, terceros o intervinientes [17].

**Partes**

Las partes en un proceso judicial informático pueden ser:

* El Ministerio Público: Es el órgano estatal encargado de la persecución de los delitos informáticos.
* El imputado: Es la persona a la que se le imputa la comisión de un delito informático.
* La víctima: Es la persona que ha sufrido un daño como consecuencia de la comisión de un delito informático.

**Terceros**

Los terceros en un proceso judicial informático pueden ser:

* Los testigos: Son las personas que pueden aportar información relevante para el proceso.
* Los peritos: Son las personas que tienen conocimientos técnicos especializados que pueden ser necesarios para el proceso.

**Intervinientes**

Los intervinientes en un proceso judicial informático pueden ser:

* Los abogados defensores: Son los profesionales que representan a las partes en el proceso.
* Los procuradores: Son los profesionales que representan a las partes en el proceso en ausencia de los abogados.

En el caso de los procesos judiciales informáticos, las partes principales son el Ministerio Público y el imputado. El Ministerio Público tiene la función de perseguir los delitos informáticos, mientras que el imputado es la persona a la que se le imputa la comisión de un delito informático [17]. Los terceros en un proceso judicial informático pueden ser las víctimas, los testigos o los peritos. Las víctimas son las personas que han sufrido un daño como consecuencia de la comisión de un delito informático. Los testigos son las personas que pueden aportar información relevante para el proceso. Los peritos son las personas que tienen conocimientos técnicos especializados que pueden ser necesarios para el proceso[14].

Los intervinientes en un proceso judicial informático pueden ser los abogados defensores y los procuradores. Los abogados defensores son los profesionales que representan a las partes en el proceso. Los procuradores son los profesionales que representan a las partes en el proceso en ausencia de los abogados [18].

# **Conclusión**

En resumen, el concepto de derecho se destaca como un conjunto de normas que rigen la convivencia bajo principios de justicia y equidad. En cuanto a los delitos informáticos en Ecuador, se evidencia una creciente preocupación debido al aumento de estos crímenes, impulsado por la accesibilidad a asesoramiento en línea. La clasificación de estos delitos abarca desde fraudes financieros hasta sabotajes informáticos y virus, destacando la necesidad de legislación más rigurosa y actualizada. El impacto de los delitos informáticos trasciende la seguridad digital, afectando negativamente la economía del país. La sofisticación creciente de los ciberataques subraya la urgencia de fortalecer medidas de seguridad, investigar casos específicos y concienciar a la sociedad sobre la importancia de la ciberseguridad.

Los delitos informáticos en Ecuador son un problema creciente, tal como ocurre en todo el mundo. Si bien se ha registrado un aumento en la discusión y el registro de casos, la falta de denuncias y la ausencia de una cultura de reporte dificultan la comprensión real de la magnitud del problema. El hecho de que Ecuador sea el tercer país con mayor incidencia de delitos informáticos en América Latina, según datos de la ONU, sugiere la necesidad urgente de implementar estrategias para fomentar la denuncia y fortalecer la seguridad cibernética. La realidad de estos ataques, junto con la evolución constante de las tecnologías, resalta la importancia de desarrollar políticas y mecanismos de prevención efectivos que protejan a las entidades públicas y privadas y fortalezcan la resiliencia digital del país.

# **Referencia**

[1] F. M. Larriva Gonzales, “El derecho Informático en la legislación Ecuatoriana,” 2006.

[2] J. C. Cadme Arcentales, “Los delitos informáticos en el Ecuador, análisis comparativo con la legislación de Colombia,” 2020.

[3] M. Fernando, S. Salgado, J. Luis, R. Villafuerte, L. Darío, and P. Salazar, “Conceptual analysis of computer crime in ecuador”.

[4] J. D. Holguín Mendoza, “Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática.,” 2021.

[5] G. J. Larreátegui Ponce, “Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso.,” 2021.

[6] S. Batra, M. Gupta, J. Singh, D. Srivastava, and I. Aggarwal, “An empirical study of cybercrime and its preventions,” in *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 42–46. doi: 10.1109/PDGC50313.2020.9315785.

[7] M. J. Chévez Morán, “Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones.,” 2021.

[8] C. Janeth, G. Bucheli, and M. J. Llerena, “Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático,” 2021, Accessed: Dec. 15, 2023. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/20319

[9] A. Yarali and F. G. Sahawneh, “Deception: Technologies and Strategy for Cybersecurity,” *Proceedings - 4th IEEE International Conference on Smart Cloud, SmartCloud 2019 and 3rd International Symposium on Reinforcement Learning, ISRL 2019*, pp. 110–120, Dec. 2019, doi: 10.1109/SMARTCLOUD.2019.00029.

[10] I. Arpaci and O. Aslan, “Development of a Scale to Measure Cybercrime-Awareness on Social Media,” *Journal of Computer Information Systems*, vol. 63, no. 3, pp. 695–705, May 2023, doi: 10.1080/08874417.2022.2101160.

[11] J. Sandage and others, “Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime.” 2013. Accessed: Dec. 16, 2023. [Online]. Available: https://www.unodc.org/documents/organized-crime/UNODC\_CCPCJ\_EG.4\_2013/CYBERCRIME\_STUDY\_210213.pdf

[12] O. Flor-Unda, F. Simbaña, X. Larriva-Novo, Á. Acuña, R. Tipán, and P. Acosta-Vargas, “A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America,” *Informatics*, vol. 10, no. 3, p. 71, Aug. 2023, doi: 10.3390/informatics10030071.

[13] R. R. Izurieta *et al.*, “Prototype to Identify the Capacity in Cybersecurity Management for a Public Organization,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 8, no. 1, pp. 108–115, Feb. 2023, doi: 10.25046/aj080113.

[14] M. Fernando, S. Salgado, J. Luis, R. Villafuerte, L. Darío, and P. Salazar, “CONCEPTUAL ANALYSIS OF COMPUTER CRIME IN ECUADOR,” 2021.

[15] B. Custers and G. Malgieri, “Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data,” *Computer Law & Security Review*, vol. 45, p. 105683, Jul. 2022, doi: 10.1016/j.clsr.2022.105683.

[16] S. M. T. Toapanta, I. N. C. Ochoa, R. A. N. Sanchez, and L. E. G. Mafla, “Impact on Administrative Processes by Cyberattacks in a Public Organization of Ecuador,” in *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, IEEE, Jul. 2019, pp. 270–274. doi: 10.1109/WorldS4.2019.8903967.

[17] L. Mayer Lux, “EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS,” *Revista chilena de derecho*, vol. 44, no. 1, pp. 261–285, Apr. 2017, doi: 10.4067/S0718-34372017000100011.

[18] D. Neufeld, “Computer crime motives: Do we have it right?,” *Sociol Compass*, vol. 17, no. 4, p. e13077, Apr. 2023, doi: 10.1111/soc4.13077.