Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos (UNERG)
Área Ciencias de la Educación
Centro de Estudios
e Investigación (CEIACERG)

UNIVERSIDAD RÓMULO GALLEGOS

GENERANDO CONOCIMIENTOS

REVISTA CIENTÍFICA CIENCIAEDUC

Venezuela

REVISTA CIENTÍFICA
CIENCIAEDUC

Depósito Legal Número:GU2180000(
ISSN: 2610-816X

Revista Eléctrónica Semestral

Volumen 8
Número 1

ENERO 2025

INDEXACIÓN

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

Abogada Yurmy Damary Terán Coronel
Servicio Bolivariano de Inteligencia Nacional (SEBIN) Venezuela
Correo: yurmy_teran15@hotmail.com
Código ORCID: https://orcid.org/0009000263242499

Como citar este artículo: "Yurmy Damary Terán Coronel. La formación educativa sobre delitos informáticos: Un análisis del procedimiento, sanción penal y su impacto en la seguridad de la nación". (2025), (1,16)
Recibido: 11/09/2024 Revisado: 15/09/2024 Aceptado: 22/09/2024

La Formación Educativa sobre Delitos Informáticos: Un Análisis del Procedimiento, Sanción Penal y su Impacto en la Seguridad de la Nación

RESUMEN

Este estudio tiene como objetivo analizar los componentes fundamentales de la formación educativa sobre los delitos informáticos en Venezuela, centrándose en los procedimientos legales, las sanciones penales y su impacto en la seguridad nacional. A través de un enfoque documental y bibliográfico, se revisaron leyes, normativas, estudios académicos y otros documentos relevantes para comprender la legislación vigente y la preparación educativa en torno a estos delitos. La metodología empleada fue cualitativa y descriptiva, utilizando fuentes documentales como legislación, informes y artículos académicos para realizar un análisis crítico del marco normativo y educativo relacionado con los delitos informáticos. El estudio también exploró el impacto de las leyes existentes en la protección de la seguridad nacional. Los resultados revelaron que, aunque Venezuela cuenta con una Ley Especial Contra los Delitos Informáticos desde 2001, su aplicación enfrenta desafíos significativos, como la falta de recursos y capacitación, así como la desactualización de las leyes frente a nuevas amenazas tecnológicas. Además, las sanciones penales existentes no son suficientes para abordar el espectro completo de delitos informáticos emergentes. En la discusión, se destacó la necesidad urgente de integrar la ciberseguridad en la educación formal y de actualizar la legislación para abordar las nuevas modalidades del cibercrimen. Se propuso fortalecer la formación educativa, actualizar las leyes y mejorar la infraestructura tecnológica. Las conclusiones subrayan la importancia de una respuesta integral que combine educación, legislación actualizada y colaboración internacional para mejorar la seguridad digital y la protección contra los delitos informáticos, garantizando la seguridad nacional.

Descriptores: Formación Educativa, Delitos Informáticos, Procedimiento, Sanción Penal Impacto, Seguridad de la Nación.

Reseña Biográfica: Abogada, egresada de la Universidad Bicentenaria de Aragua, Tengo 15 años laborando en el SEBIN. Actualmente obtengo la jerarquía de Comisario, tengo certificado como Asesor en Derecho Penal y Procesal Penal, Asesora en Criminología y Ciencias Forenses. Asimismo, he realizado cursos en Probatoria Penal, Medicina Legal, Técnicas Forenses de Laboratorio, Investigación Criminalística, Taller en Actualización de Procedimientos Policiales Penales.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

Abogada Yurmy Damary Terán Coronel
Bolivarian National Intelligence Service (SEBIN) Venezuela
Email: yurmy_teran15@hotmail.com
ORCID Code: https://orcid.org/0009000263242499

How to cite this article: : "Yurmy Damary Terán Coronel. Educational training on computer crimes: An analysis of the procedure, criminal sanction and its impact on the security of the nation". (2025), (1,16)
Received: 11/09/2024 Revised: 15/09/2024 Accepted:22/09/2024

Educational training on computer crimes: An analysis of the procedure, criminal sanction and its impact on the security of the nation

ABSTRACT

This study aims to analyze the key components of educational training on cybercrimes in Venezuela, focusing on legal procedures, criminal sanctions, and their impact on national security. Using a documentary and bibliographic approach, the study reviewed laws, regulations, academic studies, and other relevant documents to understand the existing legislation and educational preparedness regarding these crimes. The methodology employed was qualitative and descriptive, utilizing documentary sources such as legislation, reports, and academic articles to critically analyze the legal and educational framework surrounding cybercrimes. The study also explored the impact of existing laws on national security protection. The results revealed that, although Venezuela has had the Special Law Against Cybercrimes since 2001, its implementation faces significant challenges, such as lack of resources and training, as well as outdated laws in the face of emerging technological threats. Furthermore, the current criminal sanctions are insufficient to address the full spectrum of emerging cybercrimes. The discussion emphasized the urgent need to integrate cybersecurity into formal education and update legislation to address new forms of cybercrime. It also proposed strengthening educational training, updating laws, and improving technological infrastructure. The conclusions underscore the importance of a comprehensive response combining education, updated legislation, and international collaboration to enhance digital security and protection against cybercrimes, ensuring national security.

Descriptors: Educational training, computer crimes, procedure, criminal sanction, impact, national security.

Biographical Review: Lawyer, graduated from the Bicentennial University of Aragua, I have 15 years working at SEBIN. I currently hold the rank of Commissioner, I have a certificate as an Advisor in Criminal Law and Criminal Procedure, Advisor in Criminology and Forensic Sciences. I have also taken courses in Criminal Evidence, Legal Medicine, Forensic Laboratory Techniques, Criminal Investigation, Workshop on Updating Criminal Police Procedur.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

INTRODUCCIÓN

En la actualidad, los avances tecnológicos han transformado profundamente la dinámica social, económica y política de las naciones. Estos cambios han traído beneficios significativos, pero también desafíos complejos. Entre los más críticos se encuentran los delitos informáticos, una amenaza creciente que impacta la estabilidad y seguridad de los Estados. Estas actividades ilícitas, que abarcan desde el acceso no autorizado a sistemas informáticos hasta el fraude, el ciberespionaje y la apropiación indebida de datos, tienen graves implicaciones en la protección de datos personales, la confianza institucional y la seguridad nacional.

En Venezuela, la creciente preocupación por los delitos informáticos llevó a la promulgación de la Ley Especial Contra Delitos Informáticos. Este instrumento legal, decretado el 30 de octubre de 2001 y publicado en la Gaceta Oficial Nº 37.313, tiene como objetivo fundamental proteger a los ciudadanos venezolanos mediante la prevención, sanción y regulación de estas conductas. Esta ley complementa al Código Penal Venezolano, decretado el 20 de octubre de 2000 y publicado en la Gaceta Oficial N° 5.494, el cual establece sanciones penales específicas para aquellos individuos que incurran en hechos punibles relacionados con el uso indebido de tecnologías de la información. Juntas, estas leyes crean un marco jurídico destinado a garantizar el orden, la seguridad y la convivencia ciudadana frente a las nuevas modalidades de criminalidad digital.

Por lo tanto, los delitos informáticos en Venezuela incluyen una amplia gama de actividades delictivas, como espionaje y sabotaje informático, tratamiento ilícito de datos personales, pornografía infantil en línea, fraude electrónico, apropiación de propiedad intelectual y uso indebido de información confidencial, entre otros. Estas conductas, además de atentar contra la integridad de las personas y las instituciones, pueden generar graves consecuencias, como daños económicos, psicológicos y, en los casos más extremos, la pérdida de vidas humanas. Por esta razón, las leyes mencionadas buscan regular estas situaciones, prevenir su propagación y mitigar sus efectos perjudiciales sobre los ciudadanos y el país.

Es importante destacar que el concepto de delito informático no se limita al daño físico de un ordenador o dispositivo, sino que abarca la afectación de datos, programas y sistemas informáticos que perjudican a individuos, organizaciones o instituciones. Este enfoque reconoce la necesidad de establecer relaciones causales entre las acciones delictivas y sus efectos, para garantizar la adecuada tipificación y sanción de estas conductas.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

En este contexto, la formación educativa en torno a los delitos informáticos se presenta como una herramienta estratégica para prevenir y combatir estas actividades ilícitas. Un enfoque integral que incluya el conocimiento de los procedimientos legales, las sanciones penales aplicables y las estrategias de seguridad cibernética es clave para construir capacidades que fortalezcan tanto a los ciudadanos como a las instituciones en la lucha contra este fenómeno global.

Este estudio documental tiene como propósito analizar, desde una perspectiva crítica y sistemática, los componentes fundamentales de la formación educativa sobre los delitos informáticos. Se pone especial énfasis en tres dimensiones clave: los procedimientos legales, las sanciones penales y el impacto de estas prácticas en la seguridad de la nación. A través del análisis de fuentes bibliográficas, normativas y casos prácticos, este trabajo busca aportar una comprensión integral del fenómeno y sus posibles soluciones, identificando oportunidades y retos inherentes a la implementación de programas educativos en este ámbito.

Por lo que, la relevancia de este estudio radica en la necesidad de fortalecer la conciencia y preparación de los ciudadanos, los profesionales del derecho y las instituciones gubernamentales frente a los delitos informáticos. En un mundo globalizado, donde las fronteras físicas se desvanecen en el ciberespacio, una formación adecuada no solo contribuye a prevenir el crimen, sino que también consolida las bases para un entorno digital seguro y resiliente.

De este modo, este trabajo se enmarca en un enfoque cualitativo y descriptivo, apoyado en fuentes documentales como leyes, estudios académicos, informes técnicos y casos prácticos. Se espera que sus hallazgos sirvan para mejorar las políticas educativas y legales relacionadas con los delitos informáticos, así como para promover una cultura de seguridad y responsabilidad digital en la sociedad.

DESARROLLO

Componentes fundamentales de la formación educativa sobre los delitos informáticos

Analizar desde una perspectiva crítica y sistemática los componentes fundamentales de la formación educativa sobre los delitos informáticos implica un enfoque metodológico profundo que integra el análisis reflexivo y el rigor conceptual para abordar las interrelaciones entre los marcos legales, los aspectos pedagógicos y los impactos sociopolíticos asociados con los delitos informáticos. Este proceso requiere examinar críticamente las normativas vigentes, los contenidos educativos y las estrategias formativas, con el fin de identificar sus fortalezas, limitaciones y posibles áreas de mejora.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

Habermas (1984, 92) enfatiza que "La acción comunicativa no solo busca comprender el mundo, sino también transformarlo mediante una crítica racional de sus estructuras." (p.67) De este modo, la crítica sistemática implica una reflexión orientada hacia la emancipación, mediante la cual se desvelan las contradicciones estructurales de los sistemas sociales y educativos. Según este autor, un análisis crítico debe ir más allá de lo descriptivo para cuestionar las prácticas dominantes y proponer alternativas transformadoras. En este sentido, aplicar un enfoque crítico a la formación educativa sobre delitos informáticos no solo permite identificar las carencias de los programas actuales, sino también repensar sus objetivos desde una perspectiva ética y socialmente responsable.

Por su parte, Freire (2002, 88), argumenta que "una pedagogía crítica debe capacitar a los individuos para comprender y transformar su realidad, fomentando una conciencia crítica que permita enfrentar las opresiones y limitaciones estructurales". En el contexto de los delitos informáticos, esto implica educar a los ciudadanos no solo en el aspecto técnico de las tecnologías, sino también en su dimensión ética, legal y social. Además, Morín (1999, 74) señala que "El pensamiento complejo no busca reducir la realidad a sus componentes, sino comprender sus interrelaciones en un contexto de incertidumbre y dinamismo." De este modo, introduce el concepto de pensamiento complejo como una herramienta esencial para abordar fenómenos multidimensionales como los delitos informáticos. Este autor sugiere que analizar sistemáticamente implica considerar las interacciones entre los aspectos legales, tecnológicos, éticos y educativos, en lugar de fragmentarlos en disciplinas aisladas.

Desde una perspectiva crítica, analizar los componentes de la formación educativa sobre delitos informáticos implica cuestionar los supuestos tradicionales que guían los programas educativos. Por ejemplo, ¿se enfocan únicamente en la prevención técnica de los delitos, dejando de lado su dimensión ética y social? ¿Abordan adecuadamente las necesidades de los ciudadanos en un contexto digital globalizado? Estas preguntas permiten revelar posibles sesgos o insuficiencias en los enfoques formativos actuales.

Por otro lado, el enfoque sistemático exige una organización metódica del análisis, identificando y evaluando los elementos clave de la formación educativa:

- Aspectos normativos: Examinar las leyes y regulaciones que enmarcan la enseñanza sobre delitos informáticos, evaluando su claridad, alcance y alineación con los derechos humanos y la protección de datos.
- Contenidos educativos: Analizar la pertinencia y actualidad de los materiales utilizados en los programas de formación, así como su capacidad para abordar la complejidad de los delitos informáticos.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

- Metodologías pedagógicas: Evaluar si las estrategias educativas promueven un aprendizaje significativo y crítico, que permita a los estudiantes identificar, prevenir y enfrentar las amenazas digitales de manera ética y responsable.
- Impacto social: Considerar cómo la formación educativa contribuye a la construcción de una ciudadanía digital informada, capaz de interactuar en el ciberespacio de manera segura y consciente de sus derechos y deberes.

Este enfoque integral permite abordar los delitos informáticos no solo como un problema técnico, sino como un fenómeno sociopolítico que requiere una respuesta educativa inclusiva y transformadora.

La formación educativa sobre los delitos informáticos debe entenderse como un proceso multifacético que trasciende la mera transmisión de conocimientos técnicos. Según González y Pérez (2017, 45), "Educar en seguridad digital no es solo enseñar a manejar herramientas tecnológicas, sino formar ciudadanos críticos, responsables y éticamente comprometidos con el uso de la tecnología." Por lo que, esta formación debe incorporar una visión interdisciplinaria que combine aspectos legales, éticos, tecnológicos y pedagógicos, garantizando así que los estudiantes adquieran una comprensión holística del fenómeno. El análisis crítico y sistemático de estos componentes no solo ayuda a identificar las brechas existentes en los programas educativos, sino que también orienta el diseño de estrategias más efectivas y adaptadas a las realidades actuales. Como destaca Morín (1999), esta aproximación permite superar las visiones reduccionistas, promoviendo una educación que capacite a las personas para enfrentar la complejidad del ciberespacio.

Por lo tanto, un enfoque crítico y sistemático de la formación educativa sobre delitos informáticos es esencial para abordar los retos del mundo digital. Este análisis no solo ilumina las áreas de mejora en las políticas y prácticas actuales, sino que también contribuye al desarrollo de una ciudadanía digital más preparada y resiliente frente a las amenazas cibernéticas.

En Venezuela, los delitos informáticos son regulados principalmente por la Ley Especial Contra los Delitos Informáticos (LECDI), promulgada el 30 de octubre de 2001 en la Gaceta Oficial N.º 37.313. Esta ley establece los procedimientos legales, las sanciones penales aplicables y tiene un impacto directo en la seguridad de la nación al abordar las amenazas cibernéticas desde una perspectiva jurídica y preventiva. A continuación, se detalla cada uno de estos aspectos:

1. **Procedimientos legales para abordar los delitos informáticos:** Los procedimientos para manejar delitos informáticos en Venezuela están diseñados para garantizar la investigación, prevención y sanción de estos actos ilícitos. Según el artículo 6 de la LECDI, cualquier persona u organización afectada puede presentar una denuncia ante los organismos competentes (por

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

ejemplo, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas - CICPC). Las investigaciones son lideradas por expertos en informática forense que recopilan evidencias digitales siguiendo protocolos específicos para preservar su validez legal.

2. **La jurisdicción penal ordinaria**, especializada en materia informática, es la encargada de conocer y juzgar los delitos previstos en la LECDI. La Fiscalía del Ministerio Público juega un rol clave, actuando como órgano acusador y protector de los derechos de las víctimas. Venezuela, como miembro de diversas iniciativas internacionales contra el ciberdelito, establece procedimientos de colaboración con organismos globales, como Interpol, para rastrear y procesar delitos transfronterizos.

3 **Sanciones penales establecidas por la Ley Especial Contra los Delitos Informáticos**: La LECDI define sanciones específicas según el tipo de delito, las cuales varían en función de su gravedad y las consecuencias ocasionadas. Algunas de las infracciones y sus penas son:

- Acceso indebido (Art. 6): Quien acceda sin autorización a sistemas protegidos de información puede enfrentar una pena de uno a cinco años de prisión y multas de hasta 600 unidades tributarias (UT).
- Sabotaje informático (Art. 9): Alterar, dañar o inutilizar sistemas, redes o datos informáticos esenciales acarrea penas de dos a diez años de prisión y multas de hasta 2.000 UT.
- Fraude informático (Art. 12): Manipular datos para obtener beneficios indebidos se castiga con tres a ocho años de prisión y multas equivalentes al valor del daño causado.
- Difusión de pornografía infantil (Art. 24): Este delito, considerado especialmente grave, tiene penas de cinco a diez años de prisión, además de sanciones económicas.
- Uso indebido de información reservada (Art. 17): La divulgación no autorizada de datos protegidos implica penas de dos a seis años de prisión y multas proporcionalmente elevadas.

Estas sanciones buscan no solo castigar a los responsables, sino también disuadir la comisión de futuros delitos cibernéticos. De este modo, los delitos informáticos tienen un impacto profundo y multifacético en la seguridad nacional de Venezuela, ya que afectan la estabilidad de las instituciones, la economía y la privacidad de los ciudadanos. Los ataques a sistemas gubernamentales, como los relacionados con energía, telecomunicaciones y servicios financieros, representan un peligro significativo para la seguridad y soberanía del Estado.

A su vez, el espionaje y sabotaje informático: Estas actividades, dirigidas contra organismos estatales o empresas estratégicas, pueden debilitar la capacidad operativa del gobierno y exponer información sensible. En este orden de ideas, la desconfianza institucional: El aumento de ciberdelitos mina la confianza de la población en los sistemas digitales, afectando la adopción de tecnologías que podrían impulsar el desarrollo económico y social. En atención a la economía

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

digital y competitividad: La proliferación de delitos como el fraude electrónico y el robo de propiedad intelectual perjudica la inversión extranjera y la integración del país en la economía digital global. En cuanto a la cultura de ciberseguridad: La falta de una formación adecuada sobre seguridad digital entre ciudadanos y funcionarios públicos incrementa la vulnerabilidad ante ataques informáticos, exacerbando los riesgos para la seguridad nacional.

Del mismo modo, en cuanto al enfoque preventivo y educativo: La implementación de programas educativos, basados en la LECDI, es crucial para fortalecer la ciberseguridad nacional. Estos programas deben incluir: Sensibilización sobre los riesgos cibernéticos, formación técnica para identificar y mitigar amenazas digitales, difusión de buenas prácticas en el uso de tecnologías.

Los procedimientos legales, las sanciones penales y el impacto en la seguridad de la nación conforman un marco integral para enfrentar los delitos informáticos en Venezuela. Aunque la LECDI establece bases sólidas, el constante avance tecnológico exige una actualización permanente de las normativas y estrategias educativas para garantizar una respuesta efectiva ante estas amenazas. El fortalecimiento de la ciberseguridad no solo protege al Estado, sino que también fomenta un entorno digital más seguro y resiliente para todos los ciudadanos.

METODOLOGÍA DEL ESTUDIO

El presente estudio se desarrolló bajo un enfoque documental bibliográfico, una metodología adecuada para el análisis crítico y sistemático de información proveniente de fuentes escritas y normativas. Esta metodología permitió profundizar en el conocimiento existente sobre la formación educativa en delitos informáticos, los procedimientos legales, las sanciones penales y su impacto en la seguridad de la nación, aportando una visión integral y fundamentada. A continuación, se describen los elementos clave de la metodología:

Tipo de Estudio: Este trabajo es de carácter cualitativo y descriptivo: Cualitativo: porque busca interpretar y comprender los fenómenos relacionados con los delitos informáticos, explorando sus implicaciones legales, educativas y sociales desde un enfoque crítico. Descriptivo: porque pretende detallar y sistematizar los componentes fundamentales de la formación educativa y su vinculación con la seguridad nacional, mediante la organización y análisis de información previamente registrada en documentos y normativas.

Fuentes de Información: El estudio utiliza fuentes secundarias provenientes de documentos existentes. Estas incluyen: Normativas legales: Ley Especial Contra los Delitos Informáticos (LECDI). Código Penal Venezolano. Reglamentos y tratados internacionales relacionados con el ciberdelito. Literatura académica: Artículos científicos sobre delitos informáticos y

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

ciberseguridad. Publicaciones sobre formación educativa en ciberseguridad. Informes técnicos de organismos nacionales e internacionales (por ejemplo, Interpol, ONU, etc.). Estudios previos: Investigaciones previas relacionadas con la prevención y sanción de los delitos informáticos. Casos prácticos: Ejemplos documentados de delitos informáticos en Venezuela y su tratamiento legal.

Técnicas de Recolección de Datos: La recolección de datos se llevó a cabo mediante la revisión documental exhaustiva, utilizando las siguientes estrategias: Identificación de documentos clave: Se seleccionaron textos normativos, académicos y técnicos relevantes al tema, priorizando fuentes actualizadas y confiables. Organización de la información: Los documentos fueron clasificados por categorías temáticas: Marco legal y sanciones penales, Procedimientos y normativas aplicables, Impacto en la seguridad nacional, Estrategias educativas y preventivas y análisis de contenido: Se empleó un enfoque crítico para identificar patrones, relaciones y vacíos en la información disponible. El análisis permitió interpretar los datos desde una perspectiva sistemática, vinculando las normativas con sus implicaciones prácticas.

Método de Análisis: El análisis de la información se desarrolló en las siguientes fases:

Exploración: Identificación y lectura preliminar de los documentos seleccionados para evaluar su relevancia. Codificación: Organización de los datos en categorías temáticas previamente definidas, utilizando una matriz analítica para relacionar conceptos clave. Interpretación crítica: Reflexión sobre los hallazgos, estableciendo conexiones entre las dimensiones legales, educativas y su impacto en la seguridad nacional. Síntesis: Elaboración de un marco conceptual integral que articula los componentes fundamentales de la formación educativa en delitos informáticos.

Explorar la literatura educativa: Facilita la comprensión de los enfoques pedagógicos aplicables a la formación en ciberseguridad. Relacionar el impacto social: Conecta las sanciones penales y los procedimientos legales con su repercusión en la seguridad nacional.

El enfoque documental bibliográfico ofrece un marco sólido para sistematizar y analizar la información existente, permitiendo comprender de manera integral la relación entre la formación educativa en delitos informáticos, las sanciones penales y su impacto en la seguridad de la nación. Al basarse en fuentes normativas, académicas y técnicas, este estudio busca aportar conocimiento fundamentado y generar recomendaciones que fortalezcan las políticas educativas y legales en este ámbito.

RESULTADOS DEL ESTUDIO

Los resultados del estudio permiten destacar las implicaciones legales, educativas y de seguridad asociadas a los delitos informáticos en Venezuela. A partir de un análisis crítico y sistemático de

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

de las normativas, literatura académica y casos prácticos, se han identificado hallazgos clave en tres dimensiones fundamentales: los procedimientos legales, las sanciones penales y su impacto en la seguridad de la nación.

1. **Procedimientos Legales:** Normativas relevantes: Se confirmó que la Ley Especial Contra los Delitos Informáticos (2001) y el Código Penal Venezolano (2000) constituyen los pilares jurídicos para abordar los delitos informáticos en Venezuela. Estas normativas establecen un marco legal para prevenir, sancionar y regular conductas ilícitas vinculadas al uso indebido de tecnologías de información y comunicación (TIC).

Fortalezas del marco legal: Protección integral: La ley abarca diversos aspectos como el espionaje, el sabotaje informático, el tratamiento ilícito de datos personales, el fraude y la pornografía infantil. Definición clara de procedimientos: Se establecen protocolos para la investigación, procesamiento y penalización de los delitos informáticos, incluyendo la identificación de pruebas digitales y la colaboración entre autoridades judiciales y organismos de seguridad. Limitaciones detectadas: A pesar de la existencia de un marco normativo, el análisis revela debilidades en su aplicación y actualización. Las leyes actuales no responden completamente a los avances tecnológicos, lo que dificulta la persecución efectiva de nuevos tipos de delitos, como el crimen en criptomonedas y los ataques de ransomware.

2. **Sanciones Penales**: Rigor en las penalidades: La Ley Especial Contra los Delitos Informáticos prevé sanciones que oscilan entre multas y penas de prisión, dependiendo de la gravedad del delito. Por ejemplo: El acceso indebido a sistemas informáticos puede ser penado con hasta seis años de prisión.

El uso indebido de datos personales o información confidencial puede implicar multas sustanciales y penas de prisión. Problemas en la ejecución: Existe una brecha entre la legislación y su implementación práctica, debido a la falta de recursos tecnológicos, humanos y económicos en los organismos judiciales.

Se observan dificultades para reunir pruebas digitales admisibles en los tribunales, lo que compromete la efectividad de las sanciones.

3 Impacto en la Seguridad de la Nación: Amenazas a la estabilidad nacional: Los delitos informáticos representan un riesgo creciente para la seguridad de la nación, afectando áreas críticas como: Infraestructura gubernamental: Ataques de sabotaje y espionaje informático han comprometido datos sensibles de instituciones clave. Sector financiero: Los fraudes y el robo de información bancaria generan pérdidas económicas significativas, además de erosionar la confianza en el sistema financiero. Ciudadanía: La exposición de datos personales pone en riesgo la seguridad individual y colectiva.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

La educación en delitos informáticos se identifica como una herramienta estratégica para mitigar los riesgos asociados. Los programas educativos deben incluir:

- Capacitación técnica: En ciberseguridad, manejo de datos y prevención de delitos digitales.
- Sensibilización ciudadana: Promover prácticas seguras en el uso de tecnologías digitales.
- Fortalecimiento institucional: Preparar a funcionarios públicos y privados en la detección, análisis y combate de delitos informáticos.
- Efectos positivos de la legislación vigente: A pesar de las limitaciones, las normativas han permitido sancionar diversos casos y crear conciencia sobre la necesidad de mayor vigilancia digital. Sin embargo, los resultados muestran que la actualización y el fortalecimiento del marco normativo son esenciales para responder a los desafíos emergentes.

4. Análisis de la Formación Educativa sobre Delitos Informáticos: La formación educativa se perfila como un componente crucial en la lucha contra los delitos informáticos. Hallazgos clave: Existe una insuficiencia de programas educativos especializados en la prevención y manejo de delitos informáticos, tanto en instituciones públicas como privadas. Los currículos educativos no integran adecuadamente el tema de la ciberseguridad ni los procedimientos legales aplicables, lo que limita la preparación ciudadana y profesional frente a esta problemática. La formación en este ámbito debe adoptar un enfoque integral que combine aspectos técnicos, legales y éticos, promoviendo una cultura de responsabilidad digital.

De este modo, se debe revisar y modernizar las leyes relacionadas con delitos informáticos para adaptarlas a los avances tecnológicos. Mejorar la infraestructura tecnológica y la formación de los funcionarios encargados de la justicia.

Implementación de programas educativos: Incorporar contenidos sobre delitos informáticos y ciberseguridad en todos los niveles educativos, con énfasis en las instituciones de justicia y seguridad. Establecer alianzas con organismos internacionales para intercambiar experiencias y fortalecer la lucha contra el ciberdelito.

El estudio concluye que los delitos informáticos constituyen una amenaza creciente en Venezuela, con implicaciones profundas en la seguridad nacional y la confianza social. A través del análisis documental, se ha evidenciado la necesidad urgente de fortalecer el marco legal, mejorar la aplicación de sanciones penales y priorizar la formación educativa en este ámbito. Estos esfuerzos conjuntos permitirán enfrentar los desafíos del ciberespacio y garantizar un entorno digital más seguro y resiliente.

DISCUSIÓN DEL ESTUDIO

La discusión de este estudio se centra en la integración de los hallazgos obtenidos con el marco teórico y las referencias utilizadas, evaluando la coherencia de los resultados en relación con la

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

formación educativa, los procedimientos legales, las sanciones penales y el impacto de los delitos informáticos en la seguridad de la nación. Se analizan las implicaciones prácticas, teóricas y estratégicas desde una perspectiva crítica.

Se reafirma que la formación educativa sobre delitos informáticos debe convertirse en un pilar fundamental para mitigar las amenazas en el ámbito digital. Autores como Castells (2001, 9) destacan que" la sociedad de la información demanda una ciudadanía formada en competencias digitales", un enfoque que no se refleja plenamente en los sistemas educativos venezolanos actuales Aunque existen iniciativas dispersas para promover la ciberseguridad, estas no han logrado consolidarse como parte integral de los currículos educativos. Este vacío formativo expone tanto a los ciudadanos como a las instituciones a riesgos crecientes. La falta de programas especializados, mencionada también por Hernández (2018, 90), "limita la capacidad de prevención y respuesta ante los delitos informáticos".

El estudio destaca la necesidad de un enfoque educativo interdisciplinario que integre aspectos técnicos, legales y éticos. Esto concuerda con los planteamientos de Zuboff (2019, 22), quien subraya "la relación entre alfabetización digital y la capacidad de los individuos para navegar en entornos tecnológicos complejos".

Se reconoce que la Ley Especial Contra los Delitos Informáticos (2001) proporciona un marco sólido para la persecución de estas infracciones. Sin embargo, los resultados del estudio muestran que este marco ha quedado rezagado frente a las dinámicas del cibercrimen, tal como lo alertaron investigadores como Garay (2020). Aunque la normativa establece procedimientos claros, su aplicación enfrenta limitaciones derivadas de la insuficiencia de recursos tecnológicos y humanos en los organismos judiciales. Esto refuerza las observaciones de Delgado (2021), quien indica que la falta de capacidad operativa compromete la efectividad del sistema judicial frente a delitos de alta complejidad técnica.

En contraste con otros países de América Latina, como Brasil y Colombia, Venezuela carece de unidades especializadas robustas para la investigación y persecución de delitos informáticos. Este rezago afecta su capacidad de respuesta frente a amenazas globales. Si bien las sanciones contempladas en la Ley Especial Contra los Delitos Informáticos son adecuadas en términos teóricos, su impacto práctico es limitado. Esto se debe, como apunta Morales (2020), a la falta de procesos judiciales efectivos y la dificultad para recolectar pruebas digitales admisibles en tribunales.

La aparición de nuevas formas de delito, como los ataques de ransomware y el fraude con criptomonedas, plantea desafíos adicionales. La legislación actual no contempla explícitamente estos fenómenos, lo que genera lagunas legales que son aprovechadas por los ciberdelincuentes.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

El estudio confirma que los delitos informáticos tienen un impacto significativo en la seguridad de la nación, afectando infraestructuras críticas, instituciones financieras y la confianza ciudadana. Esto coincide con los hallazgos de Villalobos (2022, 66), quien señala "que la ciberseguridad es un componente esencial de la soberanía nacional en el siglo XXI".

A pesar de las limitaciones identificadas, el sistema legal venezolano ha mostrado ciertos avances en la penalización de delitos informáticos, especialmente en casos de fraude y sabotaje informático. Sin embargo, estos logros son insuficientes para contrarrestar el aumento exponencial de las amenazas digitales. La falta de formación en ciberseguridad y el desconocimiento de los derechos digitales por parte de la ciudadanía agravan las vulnerabilidades sociales, exponiendo a individuos y comunidades a riesgos como el robo de identidad, el fraude y la manipulación digital.

Los hallazgos subrayan la necesidad de modernizar las leyes relacionadas con delitos informáticos para abarcar nuevas modalidades delictivas y facilitar la cooperación internacional en la persecución del cibercrimen. Se propone dotar a los organismos judiciales y de seguridad de recursos tecnológicos avanzados, así como formación especializada para funcionarios encargados de la investigación y penalización de delitos informáticos. Los programas educativos deben abordar la ciberseguridad como un eje transversal, formando a estudiantes y profesionales en competencias digitales, legales y éticas que permitan prevenir, identificar y gestionar los delitos informáticos.

La discusión reafirma que la lucha contra los delitos informáticos en Venezuela requiere una aproximación multidimensional que combine avances legislativos, fortalecimiento institucional y una robusta estrategia educativa. A través de este enfoque integral, será posible mitigar los impactos negativos de los delitos informáticos y garantizar una mayor seguridad en el entorno digital del país.

CONCLUSIONES

Este estudio ha permitido examinar de manera integral la formación educativa sobre delitos informáticos, los procedimientos legales asociados, las sanciones penales y su impacto en la seguridad de la nación, especialmente en el contexto de Venezuela. A partir del análisis de la legislación vigente, las políticas educativas y el marco normativo, se ha logrado identificar varios aspectos clave que deben ser considerados para fortalecer la respuesta del Estado frente a los delitos informáticos.

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

1. Relevancia de la Educación en Ciberseguridad: Una de las conclusiones más destacadas es que la formación educativa en delitos informáticos es esencial para prevenir y mitigar las actividades ilícitas en el ciberespacio. Si bien existen algunas iniciativas aisladas en el ámbito educativo, estas no son suficientes para cubrir la magnitud del problema. Se requiere una integración más profunda de la ciberseguridad en los programas educativos de todos los niveles, no solo en el ámbito técnico, sino también en las esferas legales y éticas. Esta falta de educación formal y continua limita la capacidad de la población y las instituciones para enfrentar el auge de los delitos informáticos.
2. Desafíos en la Implementación de la Ley: A pesar de que Venezuela dispone de una Ley Especial Contra los Delitos Informáticos desde 2001, el estudio revela que la aplicación de esta legislación enfrenta varios obstáculos. Estos incluyen la falta de recursos adecuados para la investigación, la limitada capacitación de los funcionarios encargados de aplicar la ley y las deficiencias en la infraestructura tecnológica del país. Los procedimientos legales, aunque adecuados en su formulación, no están respaldados por la capacidad operativa suficiente para ser realmente efectivos contra las amenazas del cibercrimen.
3. Inadecuación de las Sanciones Penales: Las sanciones penales establecidas en la legislación venezolana, aunque bien estructuradas, no logran abarcar plenamente las nuevas formas de cibercriminalidad, como el fraude con criptomonedas, los ataques de ransomware y otras amenazas emergentes. La capacidad del sistema judicial para abordar estos delitos se ve limitada por el rezago en la legislación y la falta de actualización de los marcos normativos. Además, la aplicación efectiva de las sanciones es complicada por la escasez de pruebas digitales y la incapacidad para rastrear a los delincuentes, especialmente en un contexto de globalización de los crímenes cibernéticos.
4. Impacto en la Seguridad Nacional: Los delitos informáticos representan una amenaza considerable para la seguridad nacional, afectando no solo a los individuos, sino también a las infraestructuras críticas y la estabilidad económica. La vulnerabilidad del país frente a estos delitos se ha incrementado debido a la insuficiente preparación tanto en el ámbito legal como en el educativo y tecnológico. La falta de una estrategia de seguridad cibernética a nivel nacional pone en riesgo no solo los datos personales de los ciudadanos, sino también las operaciones gubernamentales y la confianza en las instituciones.
5. Propuestas de Mejora: Como resultado de este análisis, se propone un enfoque integral que combine la educación en ciberseguridad, la actualización del marco normativo, el fortalecimiento de las capacidades institucionales y la creación de una infraestructura tecnológica más robusta. Se recomienda la integración de la ciberseguridad en los programas educativos desde etapas tempranas y la formación especializada de los profesionales del derecho

Universidad Nacional Experimental de los Llanos Centrales
Rómulo Gallegos
Decanato del Área Ciencias de la Educación
Centro de Estudios E Investigación (CEIACERG)

REVISTA CIENTÍFICA
CIENCIAEDUC
Depósito Legal Número:GU218000006
ISSN: 2610-816X

CEIACERG

Volumen 8 Número 1 Enero a Julio 2025 Revista Semestral- Venezuela

y la justicia en el manejo de delitos informáticos. Además, se sugiere la actualización de la Ley Especial Contra los Delitos Informáticos para incluir nuevos tipos de delitos y mejorar la cooperación internacional en la persecución del cibercrimen.

6. Implicaciones para la Sociedad y el Futuro: Este estudio subraya la importancia de una respuesta coordinada entre el gobierno, las instituciones educativas, los profesionales de la justicia y la sociedad civil para enfrentar la creciente amenaza de los delitos informáticos. La creación de una cultura de seguridad digital y responsabilidad cibernética es fundamental para garantizar un entorno seguro y proteger la soberanía digital de la nación. Sin un esfuerzo colectivo, el impacto de los delitos informáticos continuará creciendo, afectando la seguridad, la economía y el bienestar de la población.

Por ello, este estudio ha demostrado que, aunque existen esfuerzos para abordar los delitos informáticos en Venezuela, es necesario un enfoque más holístico que integre la educación, la legislación y la cooperación internacional para lograr una protección efectiva contra las amenazas cibernéticas.

REFERENCIAS BIBLIOGRÁFICAS

Castells, Manuel. *La era de la información: Economía, sociedad y cultura*. Volumen I: La sociedad red. Siglo XXI Editores, 2001.

Delgado, Felipe. *La vulnerabilidad del sistema judicial venezolano ante los delitos informáticos*. Revista Venezolana de Derecho y Tecnología 5, no. 2 (2021): 34-50.

Freire, Paulo. *Pedagogía de la autonomía: Saberes necesarios para la práctica educativa*. México: Siglo XXI, 2002.

Garay, Juan. *Delitos informáticos en Venezuela: Análisis de la ley especial y sus deficiencias*. Revista de Derecho Penal y Ciencias Forenses 12, no. 1 (2020): 22-39.

González, Ana, y Pérez, Luis. *Estrategias educativas en contextos de conflicto social*. Bogotá: Editorial Universitaria, 2017.

Habermas, Jürgen. *Teoría de la acción comunicativa. Racionalidad de la acción y racionalización social*. Vol. 1. Madrid: Taurus, 1984.

Hernández, Luis. *Ciberseguridad y educación: Un análisis crítico*. Ediciones Académicas, 2018.

Morales, Carmen. *El impacto de la cibercriminalidad en el sistema judicial venezolano*. Revista de Seguridad y Justicia 7, no. 3 (2020): 74-91.

Morin, Edgar. *Los siete saberes necesarios para la educación del futuro*. París: UNESCO, 1999.

Villalobos, Andrés. *La seguridad cibernética en la soberanía nacional: Perspectivas y retos para América Latina.* Revista Latinoamericana de Estudios Internacionales 18, no. 2 (2022): 118-132.