Universidad Autónoma Gabriel René Moreno

Facultad de Ciencias Contables, Auditoría, Sistemas de Control de Gestión y Finanzas

Carrera Contaduría Pública

“DELITOS INFORMATICOS”

AUDITORIA DE SISTEMA DE INFORMACION Y CONTROL

Semestre 2-25 - 9no Semestre

Integrantes:

María Rosa Villalba Gonzales 218084961

David Gutiérrez Peñafiel 218150008

Profesor:

Lic. Mario Gerardo Pinto Virhuez

12 de Noviembre de 2025

RESUMEN EJECUTIVO / ABSTRACTO

El presente informe analiza el tema de los **delitos informáticos** dentro del ámbito de la **auditoría de sistemas de información**, destacando su creciente impacto en la seguridad digital de las organizaciones. En un entorno donde la tecnología es esencial para el desarrollo institucional y empresarial, las amenazas informáticas representan uno de los mayores riesgos operativos y financieros.

A lo largo del trabajo se abordan los conceptos fundamentales relacionados con los delitos informáticos, sus principales tipos, causas y consecuencias, así como las medidas preventivas que deben aplicarse mediante auditorías tecnológicas.

El estudio demuestra que la **auditoría de sistemas** cumple un rol clave en la **detección, control y prevención** de actividades ilícitas digitales, garantizando la protección de los activos de información y fomentando el uso ético de los recursos tecnológicos.

En conclusión, se resalta la necesidad de fortalecer las políticas de seguridad informática, capacitar al personal en ciberseguridad y aplicar procedimientos de auditoría que contribuyan a mitigar los riesgos derivados de los delitos informáticos

INDICE

.

RESUMEN EJECUTIVO / ABSTRACTO

El presente informe analiza el tema de los **delitos informáticos** dentro del ámbito de la **auditoría de sistemas de información**, destacando su creciente impacto en la seguridad digital de las organizaciones. En un entorno donde la tecnología es esencial para el desarrollo institucional y empresarial, las amenazas informáticas representan uno de los mayores riesgos operativos y financieros.

A lo largo del trabajo se abordan los conceptos fundamentales relacionados con los delitos informáticos, sus principales tipos, causas y consecuencias, así como las medidas preventivas que deben aplicarse mediante auditorías tecnológicas.

El estudio demuestra que la **auditoría de sistemas** cumple un rol clave en la **detección, control y prevención** de actividades ilícitas digitales, garantizando la protección de los activos de información y fomentando el uso ético de los recursos tecnológicos.

En conclusión, se resalta la necesidad de fortalecer las políticas de seguridad informática, capacitar al personal en ciberseguridad y aplicar procedimientos de auditoría que contribuyan a mitigar los riesgos derivados de los delitos informáticos.

INTRODUCCIÓN

En la actualidad, los sistemas de información se han convertido en el eje central del funcionamiento de empresas, instituciones y organismos públicos. Sin embargo, el avance de la tecnología también ha traído consigo nuevas formas de delincuencia conocidas como *delitos informáticos*, que afectan la confidencialidad, integridad y disponibilidad de la información. Estos delitos abarcan desde el robo de datos personales y financieros hasta el sabotaje digital, el fraude electrónico y la suplantación de identidad.

El estudio de los delitos informáticos dentro de la auditoría de sistemas permite identificar riesgos, evaluar controles de seguridad y promover prácticas responsables en el uso de los recursos tecnológicos. De esta manera, se contribuye a fortalecer la ciberseguridad y la confianza en los entornos digitales.

Los delitos informáticos son acciones ilícitas que se cometen mediante el uso indebido de equipos, redes o sistemas informáticos con el objetivo de causar daños, obtener beneficios económicos o acceder sin autorización a información privada. Estos delitos pueden manifestarse de diversas formas, como el robo de identidad, el fraude electrónico, la manipulación de bases de datos, la distribución de software malicioso (*malware*), el sabotaje digital o la difusión de información falsa. Cada una de estas acciones representa una amenaza directa para la seguridad de las organizaciones, afectando tanto su funcionamiento interno como su imagen pública.

.

Por tanto, el presente informe tiene como propósito analizar en profundidad el fenómeno de los **delitos informáticos**, su impacto en las instituciones y la forma en que la **auditoría de sistemas de información** puede contribuir a su prevención y mitigación. A través de este estudio se pretende fomentar una cultura de seguridad digital, ética profesional y responsabilidad tecnológica que permita proteger los activos informáticos y fortalecer la confianza en los entornos virtuales.

JUSTIFICACION

El análisis de los delitos informáticos es fundamental para comprender las amenazas que enfrentan las organizaciones en el ámbito digital. En una era donde la información es el recurso más valioso, la protección de los datos se convierte en una prioridad estratégica. Este tema se justifica porque permite desarrollar conciencia sobre los riesgos tecnológicos, mejorar los controles internos y promover políticas de seguridad adecuadas. Además, brinda a los futuros auditores de sistemas herramientas para detectar vulnerabilidades y recomendar medidas correctivas que minimicen el impacto de los ciberataques.
Por tanto, estudiar los delitos informáticos no solo es relevante para la auditoría, sino también para la gestión ética y responsable de los sistemas de información.

El estudio de los **delitos informáticos** se justifica por el acelerado crecimiento del uso de las tecnologías de la información y comunicación (TIC) en todos los ámbitos de la sociedad moderna. Actualmente, tanto las instituciones públicas como privadas dependen de sistemas informáticos para almacenar, procesar y transmitir información crítica. Sin embargo, esta dependencia también ha incrementado los riesgos relacionados con el acceso no autorizado, la manipulación de datos, el robo de información y otras actividades ilícitas que amenazan la seguridad digital.

Los delitos informáticos representan una de las mayores preocupaciones de la era tecnológica, ya que sus consecuencias pueden ser devastadoras: pérdida de información confidencial, daños financieros, interrupción de servicios y afectación de la reputación institucional. Ante esta realidad, la **auditoría de sistemas de información** se convierte en una herramienta esencial para evaluar, detectar y prevenir vulnerabilidades dentro de los entornos digitales, garantizando el cumplimiento de normas de seguridad y la correcta gestión de los recursos tecnológicos.

Analizar este tema es fundamental para comprender la importancia de establecer políticas de seguridad, controles internos y medidas preventivas que permitan minimizar los riesgos informáticos. Además, promueve la concientización sobre la responsabilidad ética en el manejo de la información y la necesidad de capacitar al personal en materia de ciberseguridad.

OBJETIVO GENERAL

El objetivo general de este informe es **analizar de manera integral el fenómeno de los delitos informáticos**, abordando su concepto, causas, tipología y consecuencias, con el fin de comprender cómo afectan la seguridad, confidencialidad e integridad de los sistemas de información dentro de las organizaciones públicas y privadas.
Asimismo, busca resaltar la **importancia de la auditoría de sistemas de información** como un proceso fundamental para la prevención, detección y control de estas actividades ilícitas que se cometen a través del uso indebido de la tecnología.

A través de este análisis, se pretende fortalecer el conocimiento sobre las amenazas informáticas más frecuentes, promover una cultura de **seguridad digital y responsabilidad tecnológica**, e incentivar la implementación de políticas, controles y procedimientos de auditoría que garanticen la protección de los activos informáticos. De esta manera, se busca contribuir al desarrollo de estrategias efectivas que permitan mitigar los riesgos cibernéticos y fomentar un uso ético, seguro y confiable de los sistemas de información en beneficio de la sociedad y las instituciones.

OBJETIVO ESPECIFICO

- ✓ Identificar los principales delitos informáticos en Bolivia.
- ✓ Analizar la legislación vigente sobre estos delitos.
- ✓ Evaluar las acciones del Estado para su prevención y sanción.
- ✓ Proponer medidas para mejorar la seguridad digital.

MARCO TEORICO

1.1 Identificación de los Principales Delitos Informáticos en Bolivia

Los delitos informáticos o ciberdelitos se definen como aquellas conductas ilícitas cometidas mediante el uso de tecnologías de la información y comunicación (TIC), con el propósito de afectar la confidencialidad, integridad, disponibilidad o propiedad de la información digital. En Bolivia, la digitalización creciente ha facilitado el acceso a sistemas y datos, pero también ha generado vulnerabilidades que los delincuentes explotan para cometer ilícitos. (González, 2023)

El Código Penal boliviano, en sus artículos 363 bis y 363 ter, establece algunos tipos de delitos informáticos, complementados por regulaciones sobre protección de datos y delitos contra la propiedad intelectual. Sin embargo, la rápida evolución tecnológica plantea desafíos para la legislación, la investigación y la prevención de estos delitos. (Quispe, 2020)

A continuación, se describen los principales delitos informáticos presentes en el contexto boliviano:

1.1.1 Acceso no autorizado a sistemas informáticos

El acceso no autorizado ocurre cuando una persona ingresa a sistemas, redes o bases de datos sin el permiso del titular. Este delito puede tener como objetivo:

- ✓ Obtener información confidencial.
- ✓ Alterar datos para beneficio propio o de terceros.
- ✓ Bloquear o destruir sistemas operativos.

1.1.2 Robo o fraude electrónico

Este delito implica la apropiación indebida de dinero, información financiera o bienes digitales mediante el uso de medios electrónicos. Entre sus modalidades destacan:

- ✓ Phishing envío de correos o mensajes fraudulentos para obtener datos personales o bancarios.
- ✓ Clonación de tarjetas: duplicación de tarjetas de crédito o débito mediante dispositivos electrónicos.
- ✓ Estafas en plataformas digitales: compras falsas, transferencias fraudulentas, etc.

Impacto social genera pérdidas económicas significativas, afecta la confianza en la banca y en las transacciones digitales y puede afectar tanto a personas como a empresas e instituciones.

1.1.3 Suplantación de identidad

La suplantación de identidad consiste en hacerse pasar por otra persona para acceder a información confidencial, realizar fraudes o causar daño a terceros. Este delito se relaciona con:

- ✓ Uso indebido de contraseñas o cuentas digitales.
- ✓ Creación de perfiles falsos en redes sociales.
- ✓ Fraudes en servicios de pago electrónico o trámites administrativos.

Importancia legal constituye una violación de derechos fundamentales como la privacidad, la intimidad y la seguridad digital, siendo perseguida por la legislación penal boliviana.

1.1.4 Difusión de malware o software malicioso

El malware es cualquier programa diseñado para dañar sistemas, robar información o alterar el funcionamiento normal de dispositivos electrónicos. Los tipos más comunes incluyen:

- ✓ Virus y troyanos alteran o destruyen archivos.
- ✓ Ransomware bloquea el acceso a datos y exige un rescate económico.
- ✓ Spyware recopila información confidencial sin consentimiento.

Consecuencias pérdida de información sensible, interrupción de servicios, daño económico y reputacional para individuos y organizaciones.

1.1.5 Ciberacoso y delitos contra la intimidad

El ciberacoso se refiere al hostigamiento, amenazas o difusión de información personal sin autorización mediante medios digitales. Incluye:

- ✓ Difusión de imágenes o videos íntimos sin consentimiento.
- ✓ Mensajes amenazantes o intimidatorios a través de redes sociales o aplicaciones de mensajería.
- ✓ Suplantación de identidad con fines de acoso.

Relevancia vulnera derechos humanos fundamentales, como la privacidad y la integridad moral de las víctimas, generando consecuencias psicológicas y sociales significativas.

1.1.6 Daño a datos o sistemas informáticos

Este delito implica la alteración, destrucción o bloqueo de información o sistemas. Puede incluir:

- ✓ Eliminación de bases de datos empresariales.
- ✓ Bloqueo de sistemas gubernamentales o institucionales.
- ✓ Modificación de información crítica para perjudicar a terceros.

Impacto afecta la operación normal de empresas, instituciones públicas y particulares, generando pérdidas económicas y sociales.

1.1.7 Importancia y contexto de los delitos informáticos

Crecimiento exponencial el aumento del acceso a internet y la digitalización de servicios públicos y privados ha incrementado las oportunidades para la comisión de ciberdelitos.

Limitaciones legales aunque el código penal boliviano tipifica algunos delitos informáticos, existen vacíos legales frente a modalidades emergentes, como ransomware, deepfakes o estafas mediante criptomonedas.

Desafíos institucionales la falta de especialización técnica de las autoridades y la insuficiente infraestructura tecnológica dificultan la investigación y sanción de los delitos.

Impacto social generan desconfianza en el uso de medios digitales, afectan derechos fundamentales y provocan pérdidas económicas considerables.

1.2 Análisis de la Legislación Vigente sobre Delitos Informáticos en Bolivia

En el contexto, la regulación de los delitos informáticos se presenta en un marco legal relativamente limitado, lo cual también implica desafíos para su aplicación efectiva. Análisis del marco normativo, sus características, alcances y vacíos principales.

1.2.1 Normativa básica aplicable

La principal norma sustantiva es el código penal de bolivia (decreto-ley 10426 de 23 de agosto de 1972) y sus modificaciones posteriores.

Mediante la ley nº 1768 del 10 de marzo de 1997, se introdujo el capítulo xi: delitos informáticos en el código penal.

Los artículos específicos incluidos son los siguientes:

Artículo 363 bis "manipulación informática" quien con la intención de obtener un beneficio indebido manipule un procesamiento o transferencia de datos informáticos, causando un resultado incorrecto y una transferencia patrimonial en perjuicio de tercero. Pena de 1 a 5 años de reclusión y multa de 60 a 200 días. (Bolivia., 2010)

Artículo 363 ter "alteración, acceso y uso indebido de datos informáticos" quien sin autorización apodere, acceda, utilice, modifique, suprima o inutilice datos en soporte informático, ocasionando perjuicio al titular de la información. Sanción: prestación de trabajo hasta 1 año o multa hasta 200 días.

También cabe mencionar que recientemente se ha aprobado la ley nº 1636 del 10 de septiembre de 2025 para la protección de la integridad sexual de niñas, niños y adolescentes en entornos digitales, lo cual complementa el régimen de delitos informáticos en un aspecto particular.

1.2.2 Relación con otros instrumentos legales y procesales

Además del régimen sustantivo penal, existen disposiciones procesales que pueden aplicarse para investigar delitos informáticos, como los artículos del código de procedimiento penal de bolivia sobre registro, incautación de datos o dispositivos informáticos.

Asimismo, la ley de 2025 (ley nº 1636) dedicada a entornos digitales para menores amplía el campo regulatorio hacia ámbitos específicos de protección en el ciberespacio. Esto indica un avance, aunque también resalta que la legislación general de delitos informáticos permanece limitada.

1.2.3 Implicaciones para la prevención y sanción

La regulación existente permite tipificar y sancionar ciertos tipos de ataques informáticos, lo que constituye una base legal para la acción del sistema de justicia.

Sin embargo, la existencia de vacíos normativos, sanciones relativamente leves y la falta de una ley especializada pueden debilitar la eficacia de la prevención, la investigación y la sanción de los ciberdelitos.

Este marco también implica que la investigación técnica, la formación de autoridades judiciales y policiales, y la cooperación internacional requieren fortalecimiento, ya que la simple existencia de normas no basta para enfrentar eficazmente el fenómeno digital.

1.2.4 Evaluación de los logros

- ✓ La CGII ofrece a entidades públicas evaluaciones de seguridad, notificaciones de vulnerabilidades y alertas de amenazas emergentes, lo cual fortalece la fase de prevención y detección temprana de incidentes.
- ✓ La cooperación internacional y los protocolos de rastreo de criptoactivos constituyen un paso importante para la fase investigativa, dado que muchos delitos informáticos trascienden fronteras y requieren coordinación internacional.
- ✓ Se evidencia una mayor visibilidad de los delitos informáticos en los medios y en estadísticas institucionales: por ejemplo, la División Cibercrimen de la Fuerza Especial de Lucha Contra el Crimen (FELCC) en La Paz recibe hasta 10 denuncias semanales de estafas, extorsión y trata en entornos digitales.

1.2.5 Limitaciones y retos importantes

A pesar de los esfuerzos, la acción estatal enfrenta desafíos críticos que limitan su eficacia en la sanción y prevención de los delitos informáticos:

- ✓ El marco legislativo es muy limitado solo dos figuras penales específicas para ciberdelitos (art. 363 bis y 363 ter) están incluidas en el código penal boliviano, lo cual deja muchas conductas emergentes sin tipificación clara.
- ✓ Las sanciones previstas son leves en muchos casos o de difícil aplicación: por ejemplo, para datos usados indebidamente (art. 363 ter) se prevé multa o prestación de trabajo hasta un año, lo que puede no ser disuasivo frente a delitos de alto impacto.
- ✓ Falta de capacidad técnica y especialización: las instituciones de investigación penal y policial perciben dificultades para acceder a datos, realizar peritajes informáticos y sostener procesos efectivos frente a ciberdelincuentes.
- ✓ Ausencia de una cultura de seguridad ciudadana y corporativa robusta: la prevención depende también del comportamiento de usuarios y empresas, lo que no siempre se encuentra suficientemente desarrollado.

Propuestas para mejorar la seguridad digital en Bolivia

La seguridad digital se define como el conjunto de políticas, procedimientos y tecnologías destinadas a proteger la información y los sistemas informáticos frente a amenazas, accesos no autorizados, daños o pérdidas. Ante el crecimiento de los delitos informáticos en Bolivia, resulta necesario analizar y proponer medidas que fortalezcan tanto la prevención como la sanción de estas conductas ilícitas. (Gutiérrez, 2022)

El fortalecimiento normativo implica la actualización del Código Penal para incluir delitos emergentes como ransomware, deepfakes, fraudes con criptomonedas y suplantación de identidad compleja, así como ajustar penas y multas para que sean proporcionales al impacto del delito y consolidar una ley de ciberseguridad integral que abarque prevención, investigación, sanción y protección de datos personales. Esto permite a las autoridades actuar de manera más efectiva y reduce los vacíos legales que los delincuentes podrían aprovechar.

El fortalecimiento institucional requiere capacitación técnica de fiscales, jueces y policías en peritaje digital, investigación de delitos cibernéticos y recuperación de evidencia digital, además de ampliar y fortalecer la CGII y la División de Cibercrimen de la FELCC con personal calificado y equipamiento moderno, así como fomentar la cooperación internacional para rastrear delitos transnacionales. Esto asegura una investigación y sanción más eficaz frente a los ciberdelitos. (Gutiérrez M. , 2023)

Las medidas preventivas y educativas incluyen campañas de concientización ciudadana sobre riesgos digitales, uso seguro de redes sociales y protección de datos personales, implementación de protocolos de seguridad informática en empresas públicas y privadas, y educación tecnológica en escuelas y universidades para crear una cultura de prevención. La prevención es más efectiva cuando usuarios y organizaciones comprenden los riesgos y adoptan medidas proactivas.

El uso de tecnología avanzada consiste en sistemas de detección de intrusiones, cifrado y autenticación de múltiples factores, y plataformas de denuncia digital con seguimiento transparente de casos. Estas herramientas reducen la vulnerabilidad de los sistemas y permiten respuestas rápidas ante incidentes.

Finalmente, la evaluación y el monitoreo continuo mediante indicadores de seguridad digital, auditorías regulares y actualización constante de políticas y herramientas garantizan que las medidas adoptadas sean efectivas frente a nuevas amenazas. La ciberseguridad es un proceso dinámico que requiere adaptación constante.

En conclusión, para reducir los delitos informáticos en Bolivia es imprescindible combinar fortalecimiento normativo, institucional, educativo y tecnológico bajo un enfoque integral y coordinado, lo que permitirá mejorar la protección de la información y los sistemas digitales, reducir la vulnerabilidad de ciudadanos, empresas e instituciones públicas, y garantizar que los delitos informáticos sean sancionados eficazmente aumentando la confianza en el entorno digital

METODOLOGÍA

La presente investigación sobre delitos informáticos en Bolivia utiliza un enfoque cualitativo, el cual permite profundizar en la comprensión de los fenómenos relacionados con la seguridad digital, la legislación vigente y las acciones estatales frente a los ciberdelitos. Este enfoque se considera el más adecuado porque los delitos informáticos no solo requieren análisis estadístico, sino también interpretación de normas, prácticas institucionales y percepciones de actores clave, como expertos en ciberseguridad, autoridades judiciales y usuarios afectados.

1.3 Tipo de investigación

El método utilizado es cualitativo, ya que la investigación se centra en comprender el fenómeno de los delitos informáticos, sus características, el marco legal vigente y la eficacia de las políticas institucionales desde una perspectiva descriptiva y analítica. Este enfoque permite explorar en profundidad los vacíos normativos, los desafíos técnicos y sociales, así como las estrategias de prevención y control aplicadas por el Estado.

La investigación es exploratoria y descriptiva, ya que busca identificar los principales delitos informáticos, analizar la efectividad de las acciones del Estado y proponer medidas de mejora en la seguridad digital. La exploración permite reconocer vacíos normativos y desafíos técnicos, mientras que la descripción aporta detalles sobre procedimientos, instrumentos legales y capacidades institucionales existentes.

1.4 Procedimiento de la investigación

Recopilación de datos:

Se realiza a través de varias técnicas complementarias:

Revisión documental y bibliográfica: análisis de leyes bolivianas relacionadas con los delitos informáticos (Código Penal y normativas complementarias), informes de organismos estatales como CGII, FELCC y Fiscalía General del Estado, y literatura académica nacional e internacional sobre ciberseguridad y delitos digitales.

Revisión de medios de comunicación y estadísticas oficiales: recopilación de casos reportados de ciberdelitos, informes de prensa y reportes de incidencia que permitan identificar patrones y tendencias.

Entrevistas semiestructuradas: diálogo con expertos en ciberseguridad, funcionarios de instituciones públicas, policías especializados y víctimas de delitos informáticos para obtener información directa y detallada sobre la situación en Bolivia.

Cuestionarios abiertos: aplicados a usuarios y organizaciones para conocer su percepción sobre la seguridad digital, experiencias con incidentes informáticos y medidas de prevención utilizadas.

1.7 Análisis de datos

Codificación y categorización: la información recopilada se organiza en categorías temáticas como tipos de delitos, medidas estatales, desafíos técnicos, vacíos normativos y propuestas de mejora.

Comparación y triangulación: se comparan los datos obtenidos de distintas fuentes para verificar consistencia, identificar contradicciones y fortalecer la confiabilidad de los resultados.

Interpretación contextual: se analiza la relación entre la legislación vigente, las acciones del Estado y la percepción de los usuarios, evaluando en qué medida estas acciones contribuyen a prevenir y sancionar los delitos informáticos.

1.5 Interpretación de resultados

Se busca establecer conclusiones sobre la efectividad de las políticas estatales y la necesidad de medidas adicionales, basadas en la evidencia recopilada y las experiencias de los actores involucrados.

Se identifican áreas críticas que requieren mejoras, como actualización normativa, fortalecimiento institucional, capacitación y educación ciudadana en seguridad digital.

1.6 Instrumentos de recolección de datos

Cuestionarios abiertos diseñados para usuarios y organizaciones, permitiendo expresar libremente experiencias, conocimientos y percepciones sobre seguridad digital.

Entrevistas semiestructuradas con expertos, autoridades y víctimas, facilitando la profundización en temas específicos y la obtención de información cualitativa rica.

Revisión documental análisis de leyes, normas, informes oficiales y literatura académica para contextualizar los hallazgos y contrastarlos con la realidad.

Análisis de contenido mediático identificación de tendencias y frecuencia de delitos informáticos reportados en Bolivia.

1.7 Justificación de la metodología

El enfoque cualitativo, junto con los instrumentos seleccionados, permite obtener una visión integral del fenómeno de los delitos informáticos en Bolivia. La combinación de fuentes documentales, entrevistas y cuestionarios asegura la triangulación de la información, aumentando la validez y confiabilidad de los resultados. Además, este enfoque facilita identificar los vacíos legales, técnicos e institucionales, así como proponer medidas concretas de prevención y mejora de la seguridad digital.

RESULTADOS

Los resultados de la investigación sobre los delitos informáticos en Bolivia se presentan en función de los hallazgos obtenidos a través de la revisión documental, entrevistas, cuestionarios y análisis de estadísticas oficiales. Estos resultados permiten comprender la situación actual, identificar vacíos y evaluar la efectividad de las acciones del Estado en materia de seguridad digital

En cuanto a los tipos de delitos informáticos más frecuentes se identificó que en Bolivia predominan las estafas electrónicas, la suplantación de identidad, los fraudes con tarjetas y cuentas bancarias, el ciberacoso, la distribución de contenidos ilegales y los delitos relacionados con datos personales. Las entrevistas con expertos y funcionarios de la FELCC indicaron que la frecuencia de estos delitos ha aumentado en los últimos años debido a la expansión del uso de internet y plataformas digitales y a la falta de cultura de seguridad digital entre usuarios y empresas

Respecto a la legislación vigente, el análisis reveló que aunque existen artículos específicos en el Código Penal como los artículos 363 bis y 363 ter, el marco legal es limitado y no contempla conductas emergentes como ataques con ransomware, fraudes con criptomonedas o delitos relacionados con deepfakes. La revisión documental y las entrevistas con abogados

y fiscales mostraron que la aplicación de las sanciones es desigual y, en algunos casos, insuficiente para disuadir a los ciberdelincuentes

Sobre las acciones del Estado y su efectividad se constató que se han desarrollado iniciativas como la creación del CGII, la División de Cibercrimen de la FELCC, protocolos de cooperación internacional y campañas de sensibilización. Sin embargo, los hallazgos indican limitaciones significativas en la capacidad técnica, la especialización del personal y la coordinación interinstitucional. Los expertos señalaron que aunque hay avances, la sanción efectiva de los ciberdelitos sigue siendo baja debido a vacíos legales y recursos limitados

La percepción de usuarios y empresas reflejó que la mayoría considera insuficientes las medidas de seguridad digital en el país. Muchos usuarios carecen de conocimientos básicos de protección de datos, manejo de contraseñas y detección de fraudes en línea. Las empresas pequeñas y medianas mencionaron que no cuentan con protocolos claros de ciberseguridad ni formación de personal, lo que aumenta la vulnerabilidad frente a ataques digitales

A partir de los hallazgos se identificaron varias medidas que podrían fortalecer la seguridad digital en Bolivia como la actualización del marco normativo para incluir delitos emergentes, el aumento de penas y sanciones disuasorias, el fortalecimiento de unidades especializadas y la capacitación técnica del personal judicial y policial, la implementación de campañas educativas masivas, el uso de tecnología avanzada como sistemas de detección de intrusiones y cifrado, y la evaluación continua de las políticas y procedimientos de seguridad digital

En síntesis los hallazgos muestran que aunque Bolivia ha avanzado en materia de prevención e investigación de delitos informáticos existen vacíos legales, limitaciones técnicas e insuficiencia en la sanción efectiva. La percepción de los usuarios y empresas confirma que la seguridad digital aún es deficiente, evidenciando la necesidad de un enfoque integral que combine normativa, institucionalidad, educación y tecnología para reducir los ciberdelitos y fortalecer la confianza en el entorno digital

ANÁLISIS E INTERPRETACIÓN DEL RESULTADO Y PROPUESTA.

Los resultados obtenidos muestran que los delitos informáticos en Bolivia han aumentado de manera significativa debido al crecimiento del uso de tecnologías digitales, la falta de cultura de seguridad entre los usuarios y las limitaciones en la prevención y sanción por parte del Estado. Los tipos de delitos más frecuentes como estafas electrónicas, suplantación de identidad, fraudes financieros y ciberacoso reflejan una vulnerabilidad generalizada tanto en ciudadanos como en empresas, especialmente en las pequeñas y medianas, que no cuentan con protocolos de seguridad ni capacitación específica.

El análisis de la legislación vigente indica que, aunque existen artículos específicos en el Código Penal que tipifican ciertos delitos informáticos, el marco normativo es insuficiente para cubrir conductas emergentes como ataques de ransomware, fraudes con criptomonedas y delitos relacionados con deepfakes. Esto limita la capacidad del Estado de sancionar de manera efectiva y disuasoria a los ciberdelincuentes. Además, la aplicación de la ley es desigual debido a la falta de especialización técnica de las autoridades, insuficiencia de recursos y coordinación limitada entre instituciones.

Las acciones estatales actuales, incluyendo la creación de la CGII, la División de Cibercrimen de la FELCC y campañas de sensibilización, son pasos importantes, pero los hallazgos revelan que aún no garantizan una prevención integral ni una sanción efectiva de los delitos informáticos. La percepción de usuarios y empresas evidencia que existe poca confianza en las medidas de seguridad digital, y una carencia de educación y conciencia sobre buenas prácticas en entornos virtuales.

La interpretación de estos resultados sugiere que para reducir los delitos informáticos en Bolivia es necesario un enfoque integral que combine fortalecimiento normativo, institucional, tecnológico y educativo. La legislación debe actualizarse para cubrir delitos emergentes y establecer sanciones proporcionales al impacto de los delitos. Las instituciones estatales requieren mayor capacitación técnica, equipamiento adecuado y coordinación entre unidades especializadas para mejorar la investigación y sanción de los delitos. Los ciudadanos y las empresas deben recibir formación continua sobre ciberseguridad, implementación de protocolos de prevención y concientización sobre el manejo seguro de la información digital.

1.8 PROPUESTAS

La propuesta se centra en cuatro ejes estratégicos:

Normativo actualizar el código penal y normativas complementarias para tipificar nuevos delitos informáticos, establecer sanciones disuasorias y consolidar una ley de ciberseguridad integral que abarque prevención, investigación y protección de datos.

Institucional fortalecer la CGII y la división de Cibercrimen de la FELCC mediante capacitación técnica de personal, equipamiento moderno y coordinación interinstitucional, además de fomentar la cooperación internacional para enfrentar delitos transnacionales.

Educativo y preventivo implementar campañas de concientización ciudadana sobre riesgos digitales, seguridad en redes y protección de datos personales; promover la educación en ciberseguridad desde escuelas hasta universidades; y exigir a empresas la implementación de protocolos de seguridad informática y formación de personal.

Tecnológico adoptar herramientas avanzadas como sistemas de detección de intrusiones, cifrado de información, autenticación de múltiples factores y plataformas de denuncia digital con seguimiento transparente de los casos, así como monitoreo y auditorías periódicas de seguridad digital en instituciones públicas y privadas.

En conclusión, la implementación de esta propuesta permitirá reducir la incidencia de delitos informáticos, mejorar la seguridad y confianza en el entorno digital, fortalecer la capacidad del estado para prevenir y sancionar delitos, y promover una cultura de ciberseguridad en la sociedad boliviana.

CONCLUSIONES Y RECOMENDACIONES

1.9 Conclusiones

La investigación sobre los delitos informáticos en Bolivia permite concluir que la creciente incidencia de ciberdelitos se debe a factores como el aumento del uso de tecnologías digitales, la falta de cultura de seguridad entre los usuarios y las limitaciones del Estado para prevenir y sancionar estas conductas. Se constató que los delitos más frecuentes incluyen estafas electrónicas, suplantación de identidad, fraudes financieros y ciberacoso, afectando tanto a ciudadanos como a empresas, principalmente a las pequeñas y medianas que carecen de protocolos de seguridad y capacitación.

La legislación vigente resulta insuficiente para cubrir delitos emergentes como ransomware, fraudes con criptomonedas o deepfakes, y su aplicación es desigual debido a limitaciones técnicas, recursos insuficientes y coordinación limitada entre instituciones. Las acciones del Estado, aunque importantes, aún no garantizan una prevención integral ni sanción efectiva, y la percepción de los usuarios evidencia una baja confianza en la seguridad digital.

El análisis confirma que para cumplir los objetivos de la investigación —identificar los principales delitos informáticos, analizar la legislación vigente, evaluar las acciones del Estado y proponer medidas de mejora— se requiere un enfoque integral que combine fortalecimiento normativo, institucional, educativo y tecnológico. La prevención, la capacitación, el uso de herramientas avanzadas y la actualización legal son elementos fundamentales para reducir la incidencia de ciberdelitos y garantizar protección y confianza en el entorno digital.

1.10 Recomendaciones

Se recomienda actualizar y ampliar la legislación boliviana para incluir delitos informáticos emergentes, establecer sanciones proporcionales al impacto del delito y consolidar una ley de ciberseguridad integral que contemple prevención, investigación y protección de datos.

Se aconseja fortalecer las instituciones encargadas de la seguridad digital, como la CGII y la División de Cibercrimen de la FELCC, mediante capacitación técnica del personal, equipamiento moderno y mayor coordinación interinstitucional, además de fomentar la cooperación internacional para enfrentar delitos transnacionales.

Es recomendable implementar campañas educativas y de concientización dirigidas a ciudadanos y empresas sobre riesgos digitales, uso seguro de internet, protección de datos personales y buenas prácticas de ciberseguridad. Asimismo, se sugiere que las empresas adopten protocolos claros de seguridad informática y capaciten a su personal de manera continua.

Finalmente, se recomienda el uso de herramientas tecnológicas avanzadas como sistemas de detección de intrusiones, cifrado de información, autenticación de múltiples factores y plataformas de denuncia digital con seguimiento transparente, así como la realización de auditorías periódicas y evaluación constante de políticas de seguridad digital para garantizar su efectividad.

Estas acciones contribuirán a reducir los delitos informáticos en Bolivia, fortalecer la protección de la información y los sistemas digitales, y promover una cultura de seguridad que aumente la confianza en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

AGETIC. (2025). *Centro de gestión de incidentes informáticos.* La Paz, Bolivia: Agencia de Gobierno Electrónico.

Arequipa Rejas, V. (2024). *La modificación del Código Penal boliviano en la incorporación de nuevos delitos informáticos.* La Paz: Juris Studia.

Bolivia, C. P. (2010). *Ley Nº 025 del Código Penal.* La Paz: Gaceta Oficial del Estado Plurinacional de Bolivia.

Bolivia., C. P. (2010). *Ley Nº 025 del Código Penal.* La Paz, Bolivia: Gaceta Oficial del Estado Plurinacional de Bolivia.

Gómez, R. (2022). El impacto de los delitos informáticos en la confianza digital. *evista Boliviana de Derecho Pena*, 34-50.

González, M. J. (2023). *Delitos informáticos y seguridad digital en Bolivia.* La Paz, Bolivia: Editorial Seguridad Digital.

Gutiérrez, M. (2022). Delitos informáticos en el Estado Plurinacional de Bolivia Desafíos legales y tecnológicos. *Revista Boliviana de Derecho y Tecnología*, 45-60.

Gutiérrez, M. (2023). Fortalecimiento institucional frente a los ciberdelitos en Bolivia. . *Revista Boliviana de Derecho y Tecnología*, 23-38.

Hernández, R. F. (2014). *Hernández, R., Fernández.* México D.F.: McGraw-Hill.

Martínez, J. P. (2018). *Comisión de delitos informáticos.* La Paz, Bolivia: Editorial Andina.

Paredes, M. (2021). *Delitos informáticos y regulación legal en Bolivia.* La Paz, Bolivia: Editorial Jurídica Andina.

Paredes, M. (2022). Fraudes electrónicos y estrategias de prevención en Bolivia. *Revista Latinoamericana de Ciberseguridad*, 6(1), 15-29.

Paredes, M. (2022). Fraudes electrónicos y nuevas modalidades delictivas en Bolivia. *Revista Latinoamericana de Ciberseguridad*, 15-29.

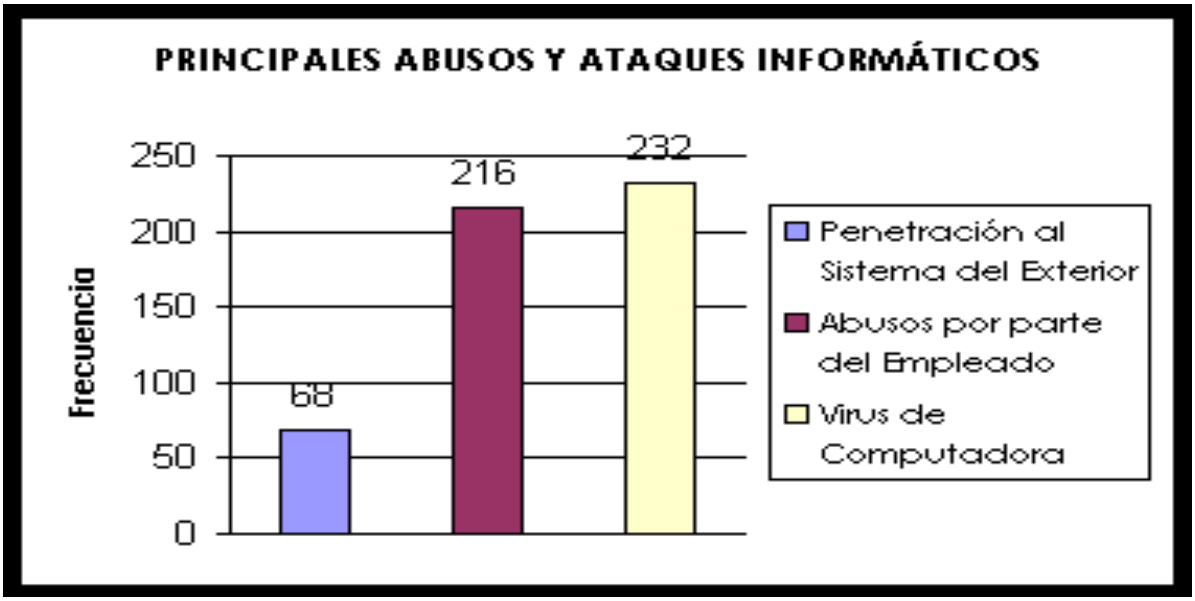
Pérez, L. (2023). *Impacto de las TIC en Bolivia:*. La Paz, Bolivia: Editorial Andina.

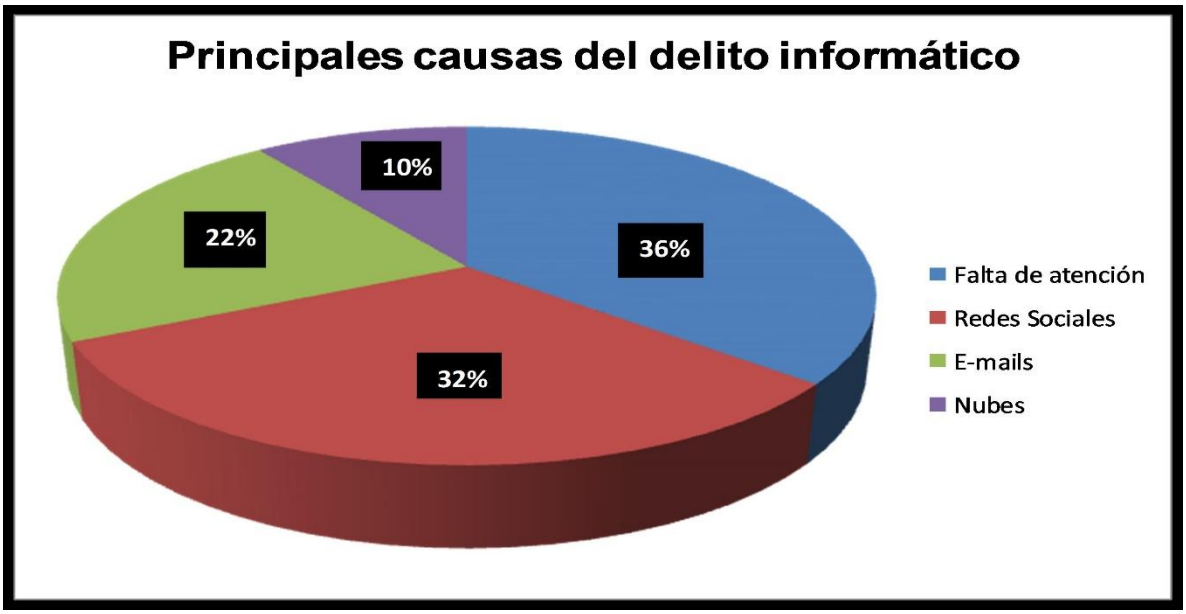
Quispe, L. (2020). Retos de la legislación boliviana frente a los delitos informáticos. . *Revista Boliviana de Derecho*, 34-50.

Torres, E. (15 de 03 de 2021). La tecnología y el aumento de los ciberdelitos. *La Razón*, págs. 12-13.

ANEXOS

- El registro puede ser realizado de forma **anónima**, pero si decide brindar su datos personales y dirección de correo recibirá una respuesta en la cual se indicarán consejos a seguir y un catálogo de profesionales especializados en asesoría legal en delitos informáticos.
- La información brindada sólo será utilizada con fines académicos, estadísticos y para asesoría general, no constituye una denuncia formal ante autoridades competentes.


PRINCIPALES ABUSOS Y ATAQUES INFORMÁTICOS
Frecuencia
250
200
150
100
50
0
68
216
232
Penetración al Sistema del Exterior
Abusos por parte del Empleado
Virus de Computadora


Principales causas del delito informático
10%
22%
36%
32%
Falta de atención
Redes Sociales
E-mails
Nubes