INSTITUTO DE INVESTIGACIÓN
CIENTIFICA, CONTABLE Y FINANCIERA
FACULTAD DE CIENCIAS CONTABLES, AUDITORÍA
SISTEMAS DE CONTROL DE GESTIÓN Y FINANZAS
UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

XIV FERIA FACULTATIVA

DE EMPRENDEDURISMO INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

NOMBRE DEL PROYECTO: **DELITOS INFORMATICOS**

CATEGORÍA

ARTÍCULOS CIENTIFÍCOS

INTEGRANTES

YARITA NUÑEZ TOMICHA 221012664

CAMILA RIBERA CRUZ 220022712

ROSITA LIMON FLORES 217105785

MARIFEL RODAS PEREZ 222003456

ALAN SAIT ARCOS CAMPOS 221008314

ERIKA GUTIERREZ BALDERRAMA 213086360

DOCENTE GUIA

LIC. MARIO GERARDO PINTO VIRHUEZ

INDICE

INTRODUCCIÓN

El desarrollo acelerado de la tecnología y el internet ha transformado profundamente la vida cotidiana, los modelos de negocio y las funciones profesionales. Sin embargo, con estos avances también han surgido amenazas que afectan la seguridad y la integridad de la información, entre ellas los delitos informáticos, también conocidos como ciberdelitos.

Los delitos informáticos son acciones ilegales que se cometen utilizando medios digitales, como computadoras, teléfonos móviles o redes de internet. También pueden tener como objetivo principal atacar o manipular sistemas informáticos, datos personales o información sensible. Lo preocupante es que, debido a la rapidez con la que evoluciona la tecnología, estos delitos también se vuelven cada vez más complejos y difíciles de detectar o prevenir.

Estos delitos abarcan una amplia gama de conductas ilícitas, como el acceso no autorizado a sistemas informáticos, el robo de datos, la suplantación de identidad, el fraude electrónico, el uso de programas maliciosos (malware). entre otros. Su impacto puede ser devastador tanto para personas naturales como para empresas y entidades públicas.

En el ámbito contable, los delitos informáticos representan un riesgo directo, ya que comprometen la privacidad de los datos financieros, pueden alterar registros contables y socavar la confianza en los informes y balances. Por eso, es fundamental que los profesionales de contaduría comprendan los riesgos tecnológicos actuales y adopten medidas preventivas.

En este trabajo se describirán los principales tipos de ciberdelitos que se presentan en la actualidad, como el malware, el phishing, el robo de identidad, el ciberacoso, entre otros. El objetivo es brindar una visión general sobre este tema para luego abordar de forma clara y estructurada la problemática de los delitos informáticos, su marco legal en Bolivia, su relación con la contabilidad y las estrategias de prevención y respuesta adecuadas.

JUSTIFICACIÓN

En la era digital, el uso masivo de tecnologías de la información y la comunicación ha traído consigo múltiples beneficios, pero también ha dado lugar a nuevas formas de criminalidad: los delitos informáticos. En Bolivia, el incremento sostenido de estos delitos, especialmente desde el año 2020, evidencia la urgencia de abordar esta problemática desde una perspectiva académica, jurídica y social.

La falta de conocimiento, la escasa legislación específica, el bajo índice de denuncias y la limitada capacidad de respuesta de las instituciones estatales han generado un escenario propicio para que estos delitos queden impunes, afectando tanto a individuos como a organizaciones. A esto se suma el desconocimiento general de la población sobre los riesgos digitales y las buenas prácticas de ciberseguridad.

El presente trabajo es necesario porque busca identificar, clasificar y analizar los principales delitos informáticos que afectan al país, sus consecuencias, su marco legal vigente y las debilidades institucionales en su tratamiento. Asimismo, pretende concienciar sobre la importancia de la prevención, el fortalecimiento de las leyes y la educación digital como herramientas fundamentales para enfrentar esta problemática.

Esta investigación es relevante no solo para el ámbito académico, sino también para la ciudadanía boliviana en general, ya que promueve la reflexión crítica sobre la seguridad digital, la protección de los datos personales y la defensa de los derechos en el entorno virtual. Con ello, se pretende aportar al desarrollo de políticas públicas eficaces, a la capacitación de los operadores de justicia y a la creación de una cultura digital responsable y segura.

OBJETIVOS

OBJETIVO GENERAL

Realizar un estudio de los delitos informáticos, sus principales características, tipos y consecuencias, con el fin de comprender su impacto en la sociedad actual, así como su regulación dentro del marco jurídico boliviano.

OBJETIVOS ESPECÍFICOS

- Definir y explicar los principales tipos de delitos informáticos que se presentan en la actualidad.
- Comprender la normativa boliviana vigente relacionada con los delitos informáticos.
- Proponer estrategias de prevención y buenas prácticas en la gestión digital de la información.

DESARROLLO EL TEMA

Un delito informático es una acción ilegal donde se utiliza la tecnología informática como medio o fin. En otras palabras, involucra el uso de computadoras, redes, software u otros dispositivos digitales para cometer actividades ilícitas.

El concepto de delitos informáticos se refiere a todas aquellas acciones ilegales o ilícitas que se llevan a cabo utilizando la tecnología informática como medio para cometer el delito o que tienen como objetivo atentar contra los sistemas informáticos, sus componentes o la información que contienen.

Clasificación de Delitos Informáticos

A. DELITOS CONTRA SISTEMAS Y DATOS

- **Acceso ilícito (hacking):** Ingresar sin permiso a computadoras, redes o cuentas.

Las puertas falsas (trap doors): Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

La llave maestra (superzapping): Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador. Su nombre deriva de un programa utilitario llamado superzap, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

Los datos falsos o engañosos (Data diddling): Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en

transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

- **Sabotaje informático:** Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Las técnicas que permiten cometer sabotajes informáticos son:

Bombas lógicas (logic bombs): Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos. Informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Gusanos: Un gusano informático es un malware que se reproduce y se propaga a través de las conexiones de red. El gusano informático no suele infectar los archivos de ordenador, sino que infecta otro ordenador de la red. Esto lo hace el gusano que se replica a sí mismo. El gusano transmite esta habilidad a su réplica, permitiéndole infectar otros sistemas de la misma manera. Aquí es también donde se encuentra la diferencia entre los gusanos informáticos y los virus. Los gusanos informáticos son programas independientes que se replican a sí mismos y se ejecutan en segundo plano,

mientras que los virus requieren un archivo de host para infectarlos. Por esta razón, es común que un gusano informático se note sólo cuando el programa está usando los recursos del sistema, ralentizando o deteniendo otras tareas.

Virus: Puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como "pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar"

Malware: Es un software diseñado intencionadamente para dañar, alterar o explotar cualquier sistema informático. No se limita a computadoras: también afecta dispositivos móviles, servidores y redes. Puede permitir a los delincuentes tomar el control de sistemas, robar información sensible, espiar a los usuarios o interrumpir procesos operativos esenciales. Su propagación puede producirse por correo electrónico, descargas desde sitios web, unidades USB, redes sociales o incluso mediante vulnerabilidades en software legítimo.

Entre las clases de malware existentes destacan:

- **Botnets:** Redes de equipos infectados que pueden usarse para enviar spam, realizar ataques DDoS o distribuir más malware.
- **Scareware:** Simula advertencias del sistema para convencer al usuario de comprar software falso.

- **Intercepción de comunicaciones (wiretapping):** Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

- **Ataques de denegación de servicio:** Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque

son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

- **Hurto del tiempo del computador:** Consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

- **Apropiación de informaciones residuales (scavenging):** Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. To scavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras 0 electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

B. DELITOS COMETIDOS MEDIANTE TIC

- **Fraude electrónico:** Estafas por internet, suplantación de páginas, phishing.

La técnica del salami (Salami Technique/Ro unc hing Down): Los actores de amenazas van transfiriendo pequeñas cantidades de dinero de la cuenta de una persona, empresa o institución a la suya propia. La clave es que estas extracciones se van haciendo en cantidades muy pequeñas y de manera espaciada, por lo que en la mayoría de los casos resultan imperceptibles para las víctimas y las entidades financieras. Los piratas informáticos pueden estar haciendo muchos ataques de este tipo de manera simultánea a miles de víctimas, por lo que la suma que van obteniendo

puede acabar siendo bastante cuantiosa para sus arcas. No obstante, también puede darse que el estafador comienza extrayendo una cantidad menor para examinar el sistema de defensa del banco y la respuesta del usuario. Si ve que no hay problemas o reclamaciones, va a más y planifica un ataque salami más complejo dirigido a aquellos que no reaccionaron al primero.

- **Falsificaciones informáticas:** Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.
- **Suplantación de identidad:** Consiste en hacerse pasar por otra persona para obtener información confidencial o cometer fraudes usando su identidad digital. Para esto se emplean diversas técnicas para obtener información personal, como el phishing o correos electrónicos falsos, y la utilización de malware, ya que luego utilizan la información recolectada para suplantar la identidad de sus víctimas, como personas naturales o empresas.

Esto puede incluir el robo de identidad, el cual implica la obtención y uso no autorizado de información personal como nombres, direcciones, números de seguro social, números de identificación de contribuyente, números de cuenta bancaria, entre otros; también puede incluir estrategias como el fraude electrónico, que es cuando un estafador utiliza la información personal robada para hacer compras, solicitar crédito o realizar otras transacciones financieras en nombre de la víctima o empresa a suplantar.

- **Pishing:** Consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario. A través de un enlace incluido en el email, intentan redirigirlo a

una página web fraudulenta para que introduzca su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca online, etc.

Estos correos electrónicos fraudulentos suelen incluir el logotipo o la imagen de marca de la entidad, pueden contener errores gramaticales y en ocasiones intentan transmitir urgencia y miedo para que el usuario realice las acciones que le solicitan.Un email de tipo phishing también puede llevar un archivo adjunto infectado con software malicioso. El objetivo de este malware es infectar el equipo del usuario y robar su información confidencial.

- **Robo de identidad:** Este delito consiste en la apropiación de datos personales (como nombre, número de identidad, dirección, claves bancarias, etc.) Para suplantar a la víctima y cometer actos ilícitos en su nombre. Esto puede derivar en la apertura de cuentas bancarias, solicitudes de crédito, compras, evasión fiscal o incluso actos delictivos más graves. Las víctimas enfrentan graves consecuencias personales y financieras, además de la dificultad de limpiar su historial.

En estos momentos también existe una nueva modalidad de Phishing que es el llamado Spears Phishing o Phishing segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

Parasitismo informático (piggybacking): El parasitismo informático permite el robo de identidad, falsificación de tarjetas de crédito, entre otros aspectos; es utilizado para acceder a sistemas privados apoyándose en virus informáticos e ingresar a servidores, modificar, manipular y apropiarse de datos confidenciales.

El proceso es sencillo, se envía a través de la red un virus informático, que cuando llega al computador de la víctima, comienza a enviar la información existente en el dispositivo huésped.

Uno de los procedimientos del parasitismo informático es alterar el sistema del computador, al instante que se activa el virus provoca cambios en la red, controlados por el maleante.

- **Espionaje informático:** Es la obtención ilícita de información protegida, a través de medios electrónicos. Suele involucrar a hackers,

competidores, o incluso estados, que acceden sin permiso a redes, bases de datos o computadoras, buscando información confidencial como secretos industriales, estrategias empresariales, datos personales, etc. Mientras que el robo o hurto de software es la apropiación no autorizada de programas informáticos. Puede ocurrir de varias formas: copiando software sin licencia (piratería), robando códigos fuente, o llevándose físicamente dispositivos que contienen programas protegidos. También incluye usar software de forma ilegal o sin pagar las licencias correspondientes.

- **Extorsión digital:** Es el uso de amenazas o chantajes mediante medios digitales para obtener dinero o beneficios. Comúnmente, los delincuentes acceden a información sensible y luego exigen pagos para no publicarla. Una variante común es el ransomware, donde se bloquea el acceso a los archivos o sistemas hasta que se pague un rescate. También se extorsiona a empresas amenazándolas con ataques informáticos o la divulgación de datos confidenciales si no pagan.
- **Ciberacoso:** Es la intimidación, hostigamiento o humillación de una persona por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. incluir insultos, amenazas, difusión de rumores, manipulación de imágenes, o incluso incitación al suicidio. Afecta especialmente a jóvenes y adolescentes, y puede tener consecuencias psicológicas graves.

Formas comunes:

- **Stalking digital:** Monitoreo persistente de la actividad de una persona.
- **Trolling:** Provocación deliberada para generar conflicto o malestar.

C. DELITOS CONTRA LA INTIMIDAD O LA DIGNIDAD

- **Violación de la intimidad:** Ocurre cuando alguien accede, difunde o utiliza sin permiso datos personales, comunicaciones privadas o información confidencial de otra persona a través de medios electrónicos (computadoras, celulares, redes sociales, correos, etc.).

Algunos ejemplos:

Empresas que rastrean la actividad del usuario para fines publicitarios sin informar adecuadamente.

Espionaje por parte de empleadores que revisan correos electrónicos o redes sociales de sus trabajadores sin justificación.

Difusión no consentida de contenido íntimo (también conocido como "porno de venganza").

Hackeo de cámaras web o micrófonos sin autorización.

- **Grooming:** Consiste en un conjunto de acciones realizadas por un adulto para establecer una relación de confianza con un menor mediante el engaño, con el objetivo de conseguir imágenes o vídeos de contenido sexual o pornográfico, e incluso llegar a establecer contacto físico con el menor para abusar sexualmente de él.

El agresor, o grooming, suele actuar detrás de un perfil falso, muchas veces haciéndose pasar por una persona de edad similar a la del menor y, para ganarse su confianza, comparte sus mismos gustos y aficiones, e incluso puede llegar a ofrecer regalos físicos o virtuales. Una vez conseguida una prueba sexual del menor (fotografía y/o vídeo) podrá usarla para chantajearle y seguir con la manipulación psicológica/emocional para obtener más material o continuar controlándolo.

- **Sextorsión:** amenaza con divulgar contenido íntimo para obtener dinero o favores.

D. DELITOS INFORMÁTICOS ORGANIZADOS

- **Distribución** de pornografía infantil.
- **Ciber terrorismo:** Se define generalmente como cualquier ataque premeditado y con motivaciones políticas contra sistemas de información, programas y datos que amenaza con violencia o la provoca. Puede incluir cualquier ciberataque que intimide o genere miedo en la población objetivo de un país, estado o ciudad, generalmente dañando o interrumpiendo infraestructura crítica vital para las operaciones sociales, económicas, políticas y comerciales.
- **Botnets y redes zombis**: redes de equipos infectados que pueden usarse para enviar spam, realizar ataques DDoS o distribuir más malware.

E. DELITOS TROYANO

Un troyano se refiere a un programa de software que parece realizar una función útil, pero en realidad realiza acciones que el usuario no desea o desconoce. Una vez instalado, el hacker puede explotar las vulnerabilidades de seguridad que crea para obtener acceso no autorizado.

Las clases de malware más utilizadas para este delito son:

- **Backdoor:** Abre una "puerta trasera" en el sistema para que el atacante acceda en cualquier momento.
- **Keylogger:** Registra todo lo que el usuario teclea, incluyendo contraseñas y mensajes privados.
- **Downloader:** Descarga otros programas maliciosos sin que el usuario lo note.
- **Banker:** Se enfoca en robar datos bancarios y de tarjetas de crédito.
- **RAT (Remote Access Trojan):** Permite el control total del equipo, incluso activar cámara y micrófono

Cómo Detectar Phishing o Pharming

- **Phishing:** Necesita engañar a la víctima con un mensaje o enlace.
- **Pharming:** No necesita que la víctima haga nada inusual; la redirección ocurre automáticamente.

Cómo detectar un intento de Phishing

a. Revisa el remitente del correo o mensaje. ¿La dirección de correo parece legítima? Muchos correos falsos usan direcciones similares a las reales, pero con errores como:

- info@seguridad-banco.com (en lugar de @bancounion.com.bo)
- Dominios extraños o letras alteradas: @gmai1.com, @faceb00k.com

b. Fíjate en el contenido del mensaje

- Urgencia sospechosa: “¡Tu cuenta será suspendida en 24 horas!”
- Premios falsos: “¡Ganaste un iPhone! Solo ingresa tus datos.”

- ❖ Errores de ortografía o redacción rara: indicio común de correos falsos.

c. Desconfía de los enlaces

- ❖ Pasa el mouse por encima del enlace (sin hacer clic). Si el destino no coincide con el texto visible, probablemente es falso.
- ❖ Ejemplo: El texto dice www.tubanco.com pero el enlace real va a http://phishingsite.ru/login.

d. No ingreses datos personales

- ❖ Bancos, empresas y gobiernos nunca te van a pedir por correo o WhatsApp tu contraseña, PIN o número de tarjeta.

e. Verifica la seguridad del sitio web

- ❖ Si llegas a un sitio desde un enlace, revisa:
- ❖ Que la dirección empiece con https:// (la "s" es de seguridad).
- ❖ Que tenga un candado en la barra de direcciones.

Cómo detectar un intento de pharming

a. Revisión de la barra de direcciones, aunque hayas escrito bien la dirección (por ejemplo, www.mibanco.bo), verifica siempre:

- ❖ Que comience con https:// (no solo http://).
- ❖ Que tenga el ícono de candado (aunque hoy en día, los atacantes también pueden usar certificados falsos).
- ❖ Que el dominio esté bien escrito y no tenga letras intercambiadas o puntos extraños (www.banc0-union.com en vez de www.banco-union.com.bo).

b. Cambios en el diseño del sitio

- ❖ Si el sitio que visitas se ve diferente a lo habitual, tiene errores visuales, faltan opciones o está mal traducido, puede ser un clon falso.
- ❖ A veces los formularios de inicio de sesión son más simples o piden más datos de lo normal.

c. Tu navegador lanza advertencia. Los navegadores modernos (Chrome, Firefox, Edge) bloquean páginas sospechosas. Si ves mensajes como:

- ❖ "Este sitio no es seguro"

- "La conexión no es privada"
- "Este sitio puede estar intentando engañarte"

Como podemos protegernos contra los delitos informáticos

a. Usa contraseñas seguras

- Combina letras, números y símbolos. No uses la misma clave en todas tus cuentas.
- Cámbialas periódicamente.

b. Activa la verificación en dos pasos (2FA)

- Agrega una capa extra de seguridad en tus correos, redes sociales y banca móvil.

c. No hagas clic en enlaces sospechosos

- Desconfía de correos, mensajes o sitios que pidan tus datos personales o bancarios.
- Revisa bien la dirección web antes de ingresar información.

d. Mantén actualizado tu antivirus y el sistema operativo

- Actualizaciones corrigen fallos de seguridad.
- Un buen antivirus detecta amenazas como troyanos, spyware y ransomware.

e. Evita redes Wi-Fi públicas para transacciones

- Si tienes que usarlas, activa una VPN.
- Preferí redes seguras y privadas para ingresar a cuentas sensibles.

f. Has copias de seguridad (backups)

- Guarda tus archivos importantes en la nube o un disco externo por si sufrís un ataque o pérdida de datos.
- No compartas tu información privada

g. Edúcate y mantente informado

- Seguí páginas oficiales como AGETIC, ASFI o la FELCC para conocer alertas y recomendaciones.

LImpacto de los delitos informáticos

Bolivia ha registrado un aumento sostenido de los delitos informáticos, especialmente a partir de 2020, con picos importantes en 2023 y 2024.Según datos de la FELCC:

En 2024, se reportaron más de 2.800 casos de ciberdelitos a nivel nacional. La mayoría ocurrió en La Paz, Santa Cruz y Cochabamba. Se estima que más del 60% de los casos no son denunciados por falta de conocimiento o confianza en el sistema.

Consecuencias:

- **Económicas**: Pérdidas de dinero directo a personas o negocios (algunas estafas superan los $us 10.000).
- **Psicológicas:** Victimización emocional, miedo, vergüenza, estrés.
- **Reputaciones:** Hackeos de empresas afectan la confianza del público.
- **Tecnológicas**: Falta de cultura digital hace que muchos bolivianos no actualicen sistemas ni usen antivirus.

Qué leyes nos protegen contra los delitos informáticos

a) Ley N° 164 de Telecomunicaciones, Tecnologías de Información y Comunicación (2011)

- **Artículo 83 y siguientes:** Define y penaliza el acceso indebido, la interceptación de datos, la interferencia en sistemas, y otros delitos relacionados con el uso de medios tecnológicos.
- Establece el marco regulatorio para el uso de redes electrónicas y promueve la seguridad informática.

b) Código Penal Boliviano (con reformas) Mediante modificaciones e interpretaciones, se han tipificado ciertos delitos informáticos bajo figuras penales como:

- **Artículo 363 bis:** Sabotaje informático
- **Artículo 363 ter:** Acceso ilícito a sistemas informáticos

- **Artículo 363 quáter:** Manipulación informática
- **Artículo 363 quinquies:** Daño o destrucción de datos o sistemas informáticos
- También se usan delitos tradicionales como la estafa (Art. 335) y la falsificación documental (Art. 198), cuando se realizan por medios informáticos.

c) **Ley N° 453** de Derechos de los Usuarios y Consumidores (2013) Protege a los ciudadanos en el uso de servicios digitales, incluyendo protección de datos personales y seguridad en las transacciones electrónicas.

d) **Ley N° 975** sobre Delitos de Racismo y toda forma de Discriminación Aplicable también en entornos digitales, como redes sociales, en casos de discriminación digital.

Como presentar una denuncia formal

a) **¿Dónde denunciar?**

- FELCC (Fuerza Especial de Lucha Contra el Crimen) – División de Delitos Informáticos.
- Ministerio Público (Fiscalía).
- Plataformas digitales oficiales de la Policía Boliviana para pre denuncias (en algunos departamentos).

b) **Qué debes llevar:**

- Tu cédula de identidad.
- Un relato detallado de lo que ocurrió.
- Toda la evidencia digital (capturas, links, mensajes).
- En casos económicos: extractos bancarios y recibos.
- Solicita apoyo legal y psicológico (si es necesario)

Legislación sobre delitos informáticos en Bolivia

En Bolivia, los delitos informáticos están regulados por el Código Penal Boliviano, con reformas introducidas en los últimos años para incluir los delitos cometidos mediante TIC. Además, el país ha trabajado en proyectos de ley específicos sobre ciberseguridad y protección de datos personales.

Algunas normativas relevantes:

- **Ley N° 164** (Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación), que contempla aspectos relacionados con la seguridad de la información.

- Propuesta de Ley de Delitos Informáticos (pendiente de aprobación), que busca tipificar específicamente una gama más amplia de ciberdelitos.

Repercusiones Sociales y Económicos

El auge de las tecnologías ha provocado un aumento considerable en la comisión de delitos informáticos, afectando tanto a personas como a organizaciones. Los costos económicos son altos y muchas veces incluyen la pérdida de información sensible, daños reputacionales, y pérdidas financieras a nivel social, también generan desconfianza en el uso de plataformas digitales.

Prevención y Gestión de Seguridad Digital

La prevención de los delitos informáticos requiere un enfoque integral que incluye:

- Educación digital y concientización de los usuarios

- Medidas técnicas como antivirus, firewalls y cifrado de datos.

- Políticas institucionales claras en torno al uso seguro de la información

- Colaboración internacional para combatir el crimen cibernético a nivel global.

Frente al crecimiento de estos delitos, es fundamental implementar estrategias de prevención, que incluyan tanto la actualización tecnológica como la concienciación de los usuarios sobre buenas prácticas de ciberseguridad. La educación digital juega un papel clave en la formación de ciudadanos responsables y conscientes de los riesgos del entorno virtual

DELITOS INFORMÁTICOS EN BOLIVIA: UN CRECIMIENTO DEL 100% EN LOS ÚLTIMOS AÑOS

1. Estafas por Internet/Suplantación de identidad (phishing, smishing, fraudes por redes sociales)

=45%

Incluye fraudes por Facebook, WhatsApp, correos falsos, suplantación de cuentas, etc.

2. Acceso indebido a sistemas informáticos (hackeos)

= 20%

Accesos no autorizados a cuentas, correos electrónicos o sistemas empresariales.

3. Extorsión digital/Sextorsión

= 15%

Casos donde se amenaza con publicar información personal o íntima a cambio de dinero.

4. Difusión de pornografía infantil/contenido ilegal

= 10%

Delitos muy perseguidos por la FELCC y la unidad de Cibercrimen.

5.Sabotaje informático y malware (virus, ransomware)

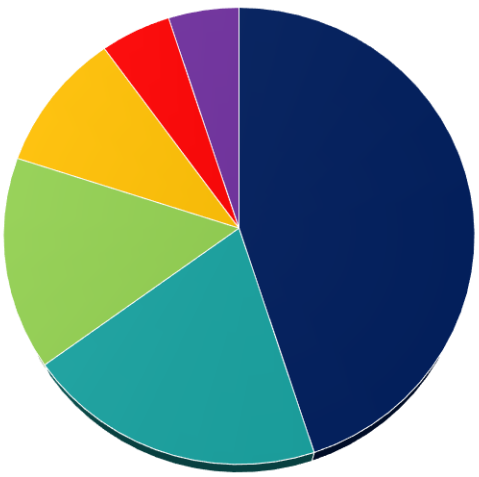
= 5%

Ataques a sistemas, especialmente en instituciones públicas o privadas.

6. Otros delitos (ciberacoso, grooming, falsificación digital, etc.)

= 5%

Incluyen conductas como el acoso por redes sociales o engaños a menor



PORCENTAJE ESTIMADO DE LOS DELITOS INFORMÁTICOS MÁS COMUNES A NIVEL GLOBAL:

1. Fraude por medios digitales (phishing, fraude en línea, estafas bancarias):

- 35-40%

(Es el más común y suele representar el mayor porcentaje de denuncias anuales)

2. Ataques de ransomware (secuestro de datos):

- 15-20%

(Particularmente en sectores críticos como salud, educación y gobierno)

3. Suplantación de identidad (identity theft):

- 10-15%

(Frecuente a través de filtraciones de datos y redes sociales)

4. Intrusión en sistemas (hacking, acceso no autorizado):

- 10-12%

(Incluye ataques a empresas, gobiernos o personas)

5. Distribución de malware (virus, troyanos, spyware):

- 8-10%

(Muchos casos están vinculados a campañas masivas de phishing)

6. Explotación infantil en línea y delitos sexuales digitales:

- 3-5%

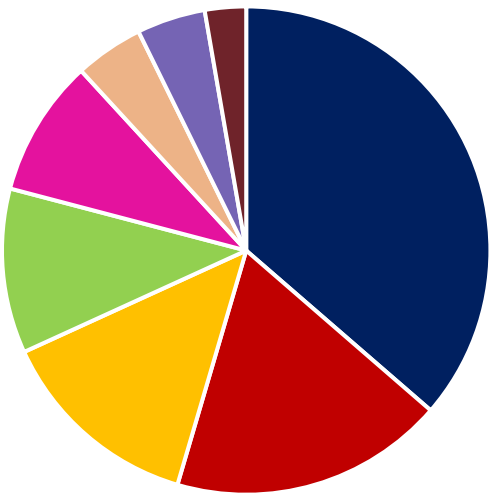
(Graves y en aumento, aunque con menor volumen que los económicos)

7. Ciberdelitos relacionados con el uso indebido de datos personales o violación de privacidad:

- 3-5%

8. Otros (amenazas en línea, acoso, ciberterrorismo, deepfakes, etc.):

- 2-3%



CAUSAS DE LA IMPUNIDAD:

- Falta de legislación específica o actualizada.
- Escasa capacitación de jueces, fiscales y policías en delitos tecnológicos.
- Carencia de laboratorios forenses digitales equipados.
- Baja cooperación internacional para rastrear delitos transnacionales.
- Temor de las víctimas a denunciar.

PORCENTAJE DE IMPUNIDAD EN LOS DELITOS INFORMÁTICOS EN BOLIVIA

La impunidad en Bolivia es un tema complejo y multifacético. Aunque no hay estadísticas precisas sobre el porcentaje de impunidad en delitos. La impunidad en delitos informáticos

DELITOS INFORMATICOS EN BOLIVIA: En 2023, el Observatorio de Delitos Informáticos de Bolivia registró 3.768 casos de delitos cibernéticos, con un aumento del 43% en estafas digitales comparado con 2022.

Los delitos más comunes incluyen fraude o estafa informática, amenazas en línea y grooming (acoso sexual digital). Los departamentos que concentran la mayor incidencia de estos delitos son La Paz, Santa Cruz y Cochabamba.

- **IMPUGNIDAD** La falta denuncia es un problema significativo, ya que la vergüenza de las víctimas, la desconfianza en la justicia y el desconocimiento en seguridad digital contribuyen a que muchos ciberdelitos queden impunes.
- **LEGISLACION**: Bolivia carece de una ley especial de delitos informáticos, y el Código Penal vigente solo contiene dos tipos penales introducidos en el 1997. Estos artículos son considerados demasiado tradicionales y no se ajustan adecuadamente a la realidad social y tecnológica del país.

PORCENTAJE DE IMPUNIDAD EN LOS DELITOS INFORMÁTICOS EN EL MUNDO

Es difícil de determinar con exactitud, pero se estima que es muy alto, con algunos estudios sugiriendo que ronda el 95%. Esto significa que, de cada 100 delitos informáticos cometidos, no llegan a ser investigados, procesados o castigados.

por ejemplo, solo se esclarece el 15% de los casos conocidos, y tan solo se investiga o detiene al 4,5% de los autores. Esto significa que la mayoría de los ciberdelitos quedan sin resolver y sin que se identifique a los responsables, lo que genera una gran sensación de impunidad entre los delincuentes

FACTORES QUE CONTRIBUYEN A LA ALTA IMPUNIDAD:

- **Dificultad para detectar y perseguir:** La naturaleza del ciberespacio hace que sea difícil rastrear y localizar a los delincuentes cibernéticos, especialmente si operan desde diferentes jurisdicciones.

- **Falta de coordinación internacional**: La ausencia de un marco legal y cooperativo efectivo a nivel global dificulta la investigación y el enjuiciamiento de delitos informáticos transnacionales.

- **Vulnerabilidades en las leyes y sistemas de justicia:** Muchas leyes y sistemas de justicia no están adaptados a la realidad del ciberespacio, lo que dificulta la investigación y la persecución de estos delitos.

- **Falta de personal especializado:** En muchos países, la falta de personal especializado en ciberseguridad dentro de las agencias de seguridad y los tribunales dificulta la investigación y el juicio de los delitos informáticos.

- **Desconfianza de las víctimas:** Víctimas de delitos informáticos no denuncian los hechos por temor a represalias o por no creer que la denuncia tendrá éxito.

- **Desconfianza en el sistema judicial:** La impunidad crea desconfianza en el sistema judicial y dificulta la protección de los derechos de las víctimas

IMPACTO DE LA IMPUNIDAD:

- **Estimula la actividad delictiva:** La alta impunidad incentiva a los ciberdelincuentes a continuar operando, lo que aumenta el riesgo de ataques y robos informáticos.

- **Disminuye la confianza en los sistemas digitales:** La alta impunidad erosiona la confianza de las personas y las empresas en la seguridad de los sistemas digitales, lo que puede afectar a la actividad económica y social.

- **Aumenta los costos de seguridad:** Para protegerse de los delitos informáticos, las empresas y las personas deben invertir en medidas de seguridad, lo que aumenta los costos.

SOLUCIONES PARA COMBATIR LA IMPUNIDAD:

- **Fortalecer la cooperación internacional:** Es necesario establecer acuerdos internacionales para facilitar la investigación y el enjuiciamiento de delitos informáticos transnacionales.

- **Aumentar el personal especializado:** Es fundamental contar con personal especializado en ciberseguridad dentro de las agencias de seguridad y los tribunales.

- **Modernizar las leyes y sistemas de justicia:** Las leyes y sistemas de justicia deben adaptarse a la realidad del ciberespacio.

- **Promover la denuncia de los delitos:** Es necesario crear mecanismos para facilitar la denuncia de los delitos informáticos y garantizar la protección de las víctimas.

- **Mayor sensibilización y educación:** Es necesario llevar a cabo campañas de sensibilización y educación para que la población conozca los riesgos de los delitos informáticos y sepa cómo denunciarlos.

CONCLUSIÓN

Los delitos informáticos representan una amenaza creciente y compleja en la era digital. A diferencia de los delitos tradicionales, estos pueden cometerse a distancia, de forma rápida y con un alto nivel de anonimato, lo que dificulta su detección, investigación y sanción. Desde fraudes como el phishing o la manipulación de datos, hasta sabotajes, espionaje, robo de software o acceso no autorizado, todos tienen en común el uso indebido de la tecnología para generar daño o beneficio ilícito.

En Bolivia representan un desafío significativo para la sociedad y el marco legal del país. son un fenómeno en ascenso que requiere una respuesta integral y coordinada. Es fundamental que el marco legal se fortalezca y que se fomenten iniciativas de educación y concienciación para enfrentar este fenómeno. Solo a través de un esfuerzo conjunto entre el gobierno, las empresas y la sociedad civil se podrá construir un entorno digital más seguro y proteger a los bolivianos de las amenazas cibernéticas.

En definitiva, los delitos informáticos exigen una respuesta coordinada entre leyes, educación, tecnología y cooperación internacional para garantizar la seguridad y los derechos en el entorno digital.

RECOMENDACIÓN

- **Cómo podríamos mejorar y proteger al ciudadano boliviano contra los delitos informáticos.**

a. FORTALECIMIENTO LEGAL

Crear una Ley Integral sobre Delitos Informáticos. Tipificar con claridad delitos como:

- Suplantación de identidad digital Grooming (acoso sexual en línea a menores)
- Ciber extorsión
- Acceso ilícito, daño informático y espionaje digital.
- Incluir medidas cautelares específicas: bloqueo de perfiles, cierre de cuentas, protección de víctimas.
- Reforma al Código Penal y Código de Procedimiento Penal
- Adaptar los procedimientos judiciales para que incluyan:
  - ✓ Pruebas digitales válidas
  - ✓ Pericias informáticas
  - ✓ Delitos transnacionales

b. FORTALECIMIENTO INSTITUCIONAL Y TECNOLÓGICO

- Modernizar y ampliar la División de Delitos Informáticos (FELCC)
  - ❖ Presupuesto específico para laboratorios de **ciber forense.**
  - ❖ Capacitación continua para policías y fiscales en análisis digital, **blockchain**, criptografía, etc.
  - ❖ Equipamiento con software de rastreo, análisis de redes y datos.
- Crear una Unidad Nacional de Respuesta Rápida a Incidentes Digitales
  - ❖ Con personal técnico, jurídico y psicológico.
  - ❖ Capaz de actuar en menos de 24 horas en casos críticos (pornografía infantil, estafas masivas, cibera coso, filtración de datos, etc.)

c) EDUCACIÓN DIGITAL Y PREVENCIÓN

- Implementar una campaña nacional de alfabetización digital en colegios, universidades, barrios y redes sociales. Contenidos como:

- ❖ Seguridad en redes sociales
- ❖ Uso responsable de internet
- ❖ Reconocimiento de estafas y **phishing**
- ❖ Manejo de contraseñas y privacidad

➢ Crear una materia obligatoria en escuelas: "Cultura Digital y Ciudadanía Cibernética"

- ❖ Desde primaria, con apoyo de educadores y expertos en ciberseguridad.

d) PROTECCIÓN CIUDADANA EFECTIVA

➢ Portal Nacional de Denuncias Digitales

- ❖ Sitio web y app móvil para denunciar delitos informáticos con evidencia.
- ❖ Sistema seguro, anónimo si se desea, con seguimiento automatizado.

➢ Defensoría Digital del Ciudadano, como oficina encargada de proteger los derechos digitales, similar a una defensoría del consumidor, con capacidad de:

- ❖ Atender quejas
- ❖ Mediar con empresas de tecnología
- ❖ Presionar por eliminación de contenido nocivo

e) COOPERACIÓN INTERNACIONAL Y PÚBLICO-PRIVADA

➢ Adherirse al Convenio de Budapest (Convenio sobre Ciberdelito)

- ❖ Facilita la cooperación entre países en investigaciones digitales.
- ❖ Acceso a asistencia técnica, capacitación y plataformas internacionales.

- Alianzas con empresas tecnológicas y bancos

  - Facebook, Google, WhatsApp, TikTok, bancos y fintech deben firmar convenios con la justicia boliviana.

  - Establecer protocolos para la protección de usuarios bolivianos.

7 ANEXOS

7.1 Anexo 1: Acceso ilícito

Descripción: Ingreso no autorizado a sistemas o redes informáticas Ejemplo real: Un hacker accede al servidor de una universidad y roba información de los estudiantes.
Descripción: Ingreso no autorizado a sistemas o redes informáticas Ejemplo real: Un hacker accede al servidor de una universidad y roba información de los estudiantes.

7.2 Anexo 2: Interceptación de comunicaciones

Descripción: Captura de datos o comunicaciones sin consentimiento.

Ejemplo real: Instalación de un software espía en una red WiFi para leer correos electrónicos ajenos.

7.3 Anexo 3: Daños informáticos (ataques a sistemas)

Descripción: Introducción de malware para dañar datos o sistemas.

Ejemplo real: Un virus que borra los archivos de una empresa o inutiliza sus servidores.

7.4 Anexo 4: Fraude informático

Descripción: Manipulación de sistemas informáticos para obtener un beneficio económico.

Ejemplo real: Un phishing bancario donde se engaña a los usuarios para que revelen datos de acceso a su cuenta.

7.5 Anexo 5: Suplantación de identidad digital

Descripción: Uso de la identidad digital de otra persona sin autorización.

Ejemplo real: Crear un perfil falso en redes sociales para acosar o estafar a otras personas.

7.6 Anexo 6: Delitos contra la propiedad intelectual

Descripción: Distribución no autorizada de software, música, películas, etc.

Ejemplo real: Compartir contenido pirata a través de plataformas P2P

.

7.7 Anexo 7: Pornografía infantil en línea

Descripción: Distribución, producción o posesión de material de abuso infantil.

Ejemplo real: Almacenamiento de imágenes ilegales en servidores ocultos de la dark web.

BIBLIOGRAFÍA

1. Bolivia. Ley No1455 ley de organización judicial, gaceta oficial del Bolivia 1993.

2. Delitos informáticos en el derecho penal contemporáneo" - Revista de Derecho Penal y Criminología (Argentina), varios números. Disponible en base de datos jurídicas como La Ley o Rubinzal

3. INTERPOL-Cybercrime

https://www.interpol.int/en/Crimes/Cybercrime Información sobre delitos digitales a nivel global.

4. ttps://es.scribd.com/document/354861989/Marco-Teorico-Delitos-Informatico

5. "La ley penal ante los delitos informáticos: un análisis crítico" de Carlos Gómez-Jara Díez.

Este artículo discute las lagunas en la legislación penal respecto a los delitos informáticos y propone soluciones.

6. Google Scholar (https://scholar.google.com/)

7. ScienceDirect (https://www.sciencedirect.com/)

WEB GRAFÍA

1. Wikipedia-Delitos Informáticos https://es.wikipedia.org/wiki/Delito inform%C3%A1tico Buena introducción general con enlaces a leyes, ejemplos y artículos relacionados.

2. Observatorio Delitos Informáticos de Latinoamérica (ODILA)

https://odila.org Iniciativa que reúne estadísticas, reportes y alertas sobre delitos informáticos en países de América Latina.

3. Chema Alonso - Blog sobre seguridad informática https://www.elladodelmal.com Blog personal de un experto en hacking ético y ciberseguridad, con casos reales y análisis técnicos.

3. Kaspersky - Noticias y consejos sobre seguridad digital https://latam.kaspersky.com/blog/Noticias actualizadas sobre amenazas cibernéticas y recomendaciones de protección.L

4. - Instituto Nacional de Ciberseguridad de España (INCIBE) – https://www.incibe.es

5. - Kaspersky Security Center – https://www.kaspersky.com/resource-center

6. - Interpol – https://www.interpol.int

7. - Europol – https://www.europol.europa.eu

8. - Comisión Federal de Comercio (FTC) – https://www.identitytheft.gov

9. - UNICEF – https://www.unicef.org

10. - Save the Children – https://www.savethechildren.es

11. - Electronic Frontier Foundation –https://www.eff.org

12. - Microsoft Security Blog – https://www.microsoft.com/security/blo

13. - Symantec Threat Report – https: //www.broadcom.com