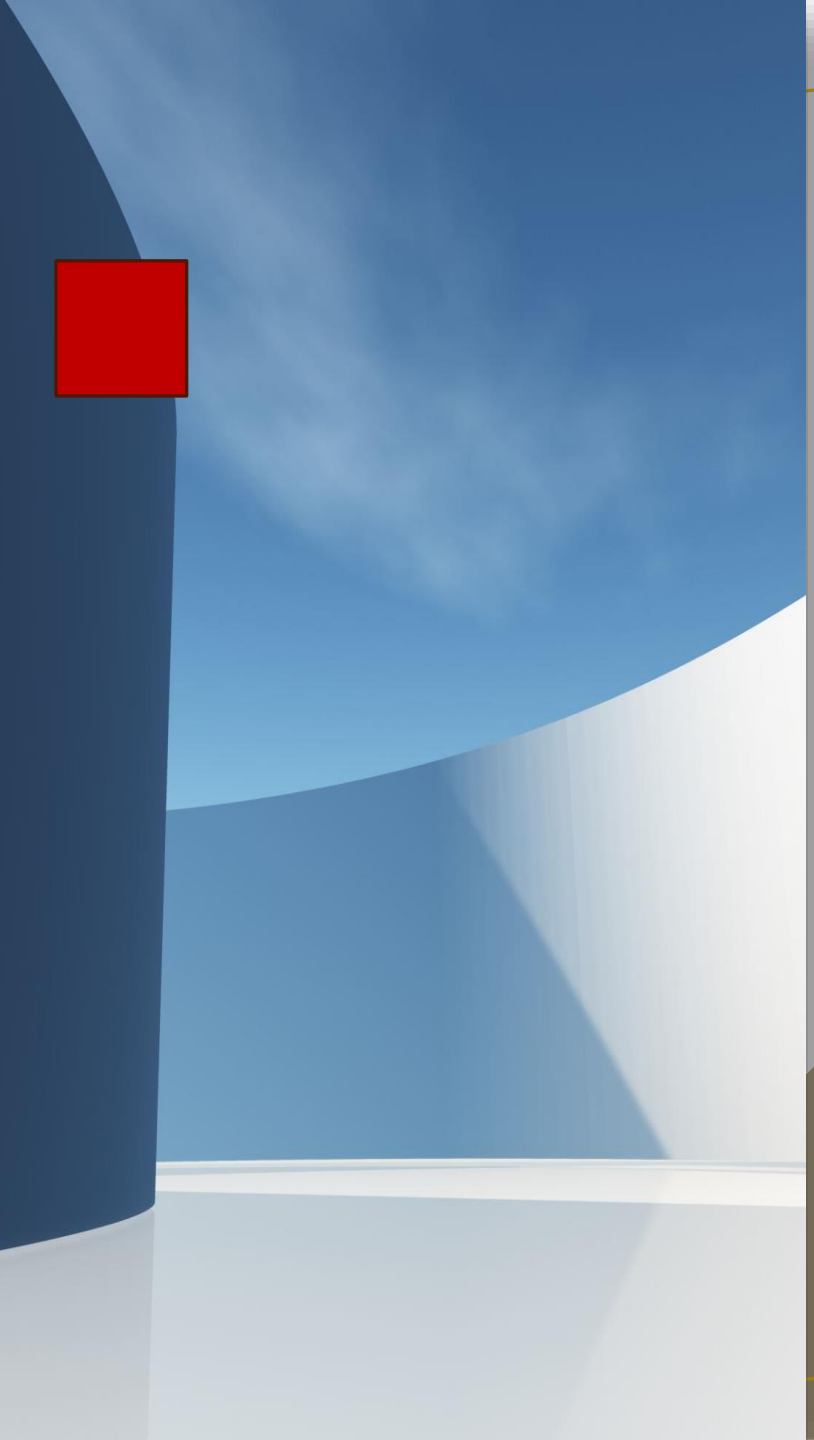
DELITOS INFORMÁTICOS

(Compilación de IA)

Alex R. Zambrano Torres



DELITOS INFORMÁTICOS

(Compilación de IA)

UNIDAD I: Introducción

- Concepto De Derecho
- Concepto de Derecho Penal
- Concepto de delito informático.

- Historia y evolución
- Actores y motivaciones de los cibercriminales.

Introducción.- Presupuestos:

- El Derecho Penal regula los daños irreparables, lo que no se puede reparar debe encontrarse regulado dentro del derecho administrativo o faltas.
- El Derecho Penal informático
- 1) El fenómeno es que son delitos de mayor alcance
- 2) Son de mayor nivel de daño al patrimonio
- 3) Son de peligro invisible
- 4) Pueden ser cometidos por niños o mayores
- 5) Son de alta complejidad
- 6) El número de delincuentes es todo el mundo
- 7) El espacio a proteger es todo el mundo
- 8) Plantea la creación y garantía de derecho digitales:
  - Derecho a la imagen digital
  - Derecho a la buena reputación digital
  - Derecho a la integridad digital
  - Derecho al secreto bancario digital
  - Derecho a la reserva de los registros digitales

Introducción

PRESUPUESTOS:

- 9) Derecho a la reserva de los datos registrados en bancos, celulares, Facebook, Instagram, internet, aplicaciones, e-mail
- 10) Regulación de la responsabilidad administrativa, civil y penal de las redes sociales
- 10) Determinación correcta de las definiciones, como por ejemplo, el phishing no es robo de identidad, sino suplantación, usurpación
- 11) En los delitos informático debe plantearse si se puede considerar como robo, aquellos que más bien son hurtos, por que no hay uso de la violencia
- 12) No existe límite por condición de lenguaje, nacionalidad, identidad cultural, idiosincrasia, etc.
- 13) Supera o desborda el margen de los límites geográficos

Introducción

PRESUPUESTOS:

- 14) Supera o desborda el margen de la soberanía estatal
- 15) Determina un nuevo tipo de autores, coautores, cómplices digitales, con nuevos personajes, hacker, crackers, grooming, etc.
- 16) Se tienen que enfrentar a un nuevo sistema u orden económico, las criptomonedas, bitcoing
- 17) Los delitos informáticos pueden clasificarse por la
  - A) autoría individual
  - B) Autoría colectiva
  - C) Autoría con participación de la víctima
  - D) Autoría con participación de la institución
- 18) En algunos tipos se requiere indispensablemente la participación de la víctima para
  - A) poner en peligro, Contagiarse a través de clickear, descargar aplicativos, etc.

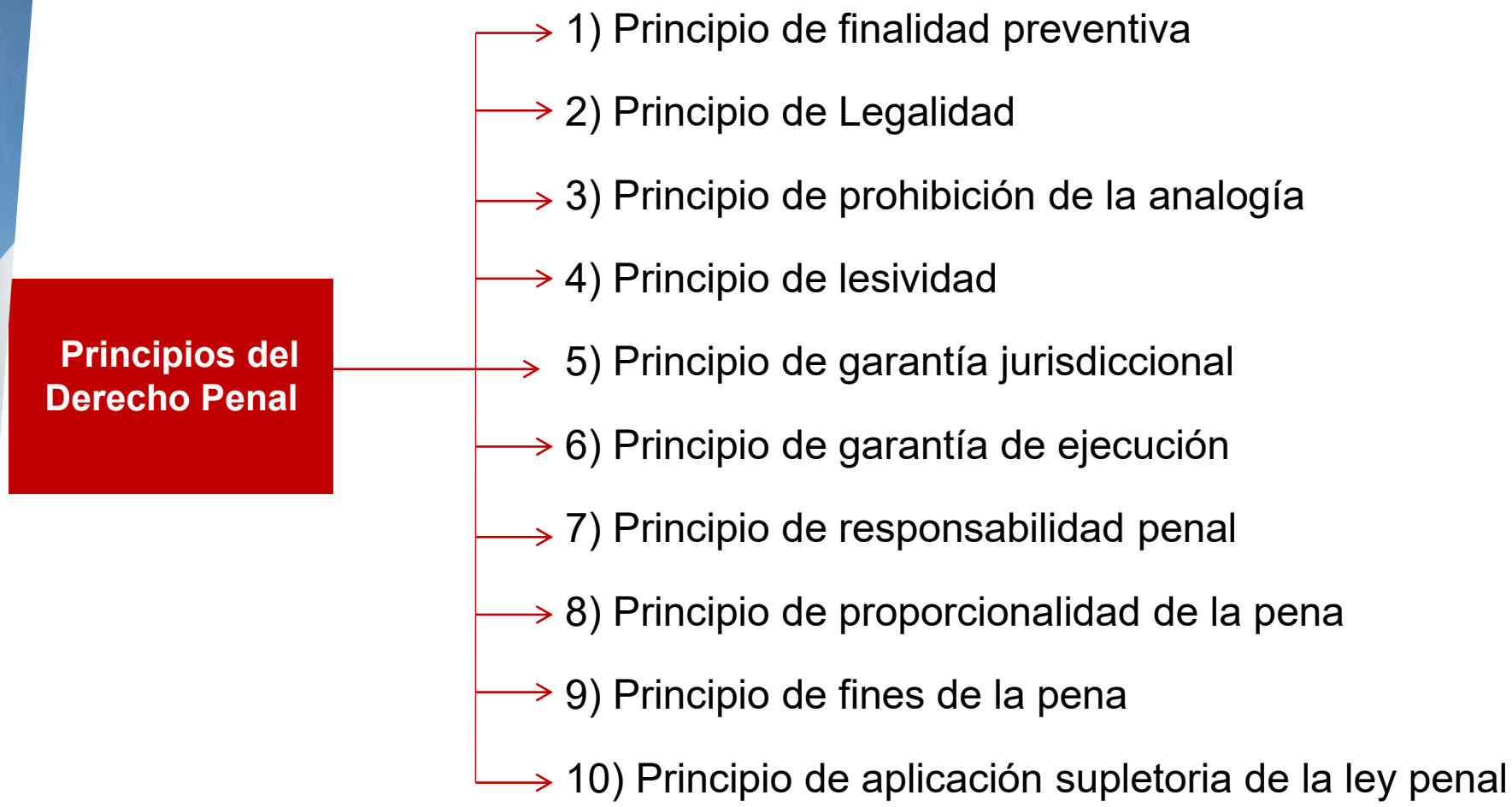
Introducción

PRESUPUESTOS:

- 19) Se evidencia la “vida digital” de las personas
- 20) los overshering, o dar mucha información al internet
- 21) Imposibilidad de asegurar la protección o seguridad

Principios del Derecho Penal.-

- Son sistemas que limitan el poder punitivo del Estado y evitan la impunidad del infractor



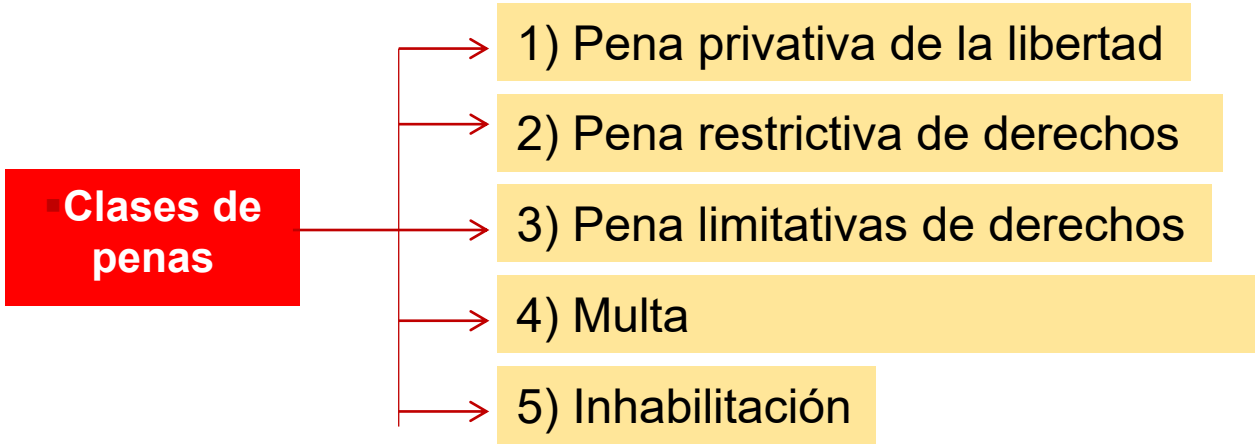
LA AUTORÍA PENAL:

Concepto de Autor:	Autor es la persona que comete el delito

- **Tipos de Autor**
  - 1) Autor
  - 2) Autor Mediato
- **Partícipes**
  - 3) Cómplice
  - 4) Cómplice primario
  - 5) Cómplice secundario

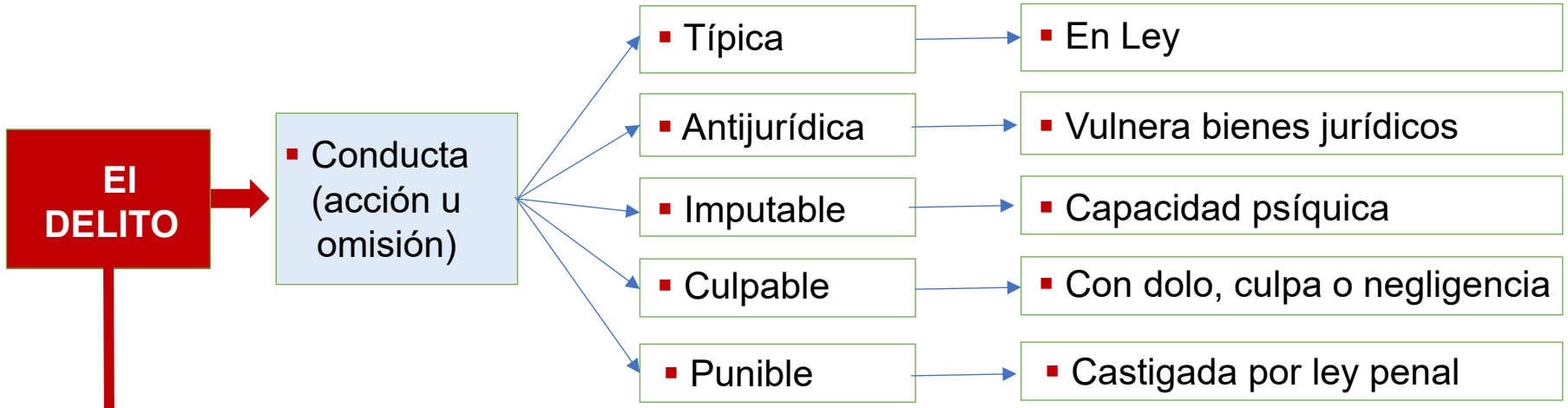
LAS PENAS.-

Concepto de penas.-	Sanción penal impuesta por el Estado punitivo a imputado



EL DELITO / Elementos constitutivos:

- El **DELITO** es una conducta (acción u omisión), típica, antijurídica, imputable, culpable y punible



- CONDUCTA PUNIBLE
- **Sistema de subordinación del individuo al Estado o sociedad**
- Sistema unitario de control social, político y económico
- Contrato de adhesión penal
- Determinación de una relación penal entre el individuo y el Estado

EL DELITO INFORMÁTICO / Concepto:

- El delito informático es toda acción ilícita, antijurídica o contraria a la **ética** que utiliza tecnologías de la información y comunicación como instrumento o medio para su comisión.
- Afectan sistemas informáticos, datos, la privacidad, seguridad o integridad de personas, empresas o instituciones.
- Regulada por la Ley N 30096 - Ley de Delitos Informáticos;
- El delito informático es cualquier infracción penal cometida mediante el uso de sistemas informáticos o tecnologías digitales, que busque un beneficio ilícito o cause perjuicios a terceros.
- Puede involucrar accesos ilegales a sistemas, daño o alteración de datos o sistemas, interceptación de comunicaciones, fraude, suplantación de identidad, entre otros.
- Los sistemas informáticos pueden ser tanto el objeto material (p.ej., bases de datos, servidores) como el instrumento para cometer el delito.
- Estos delitos se tipifican no solo por el medio usado, sino por la necesidad del conocimiento informático para su ejecución, investigación y persecución.
- Además, el delito informático difiere de otros crímenes tradicionales porque involucra la dimensión digital, con retos específicos como la localización espacial y temporal del acto, la cadena de custodia digital y la defensa de derechos fundamentales en el entorno digital.

EL DELITO INFORMÁTICO:

- El **DELITO** es una conducta (acción u omisión), típica, antijurídica, imputable, culpable y punible

El DELITO

- Típica, Antijurídica, Imputable, Culpable, Punible
- **CONDUCTA** (acción u omisión)
  - A través de medios digitales, informáticos, electrónicos
    - Medios de comunicación
      - E-mail
      - Mensajería
      - WhatsApp
      - Telegram
    - Redes sociales
      - Facebook
      - Instagram
      - TikTok
    - Sistemas de transferencia financiera
      - Tarjetas bancarias
      - DNI electrónicos
      - Yape
      - Plin
      - Visa
    - Registros de identidad
      - Registro biométrico
      - Registro visual
      - IP
      - I Cloud

Historia de los Delitos Informáticos.-

- Antes de la existencia del internet, ya existían delitos relacionados con el uso indebido de tecnologías como el telégrafo y las redes telefónicas.
- Un caso temprano de fraude tecnológico ocurrió en 1824 con el hackeo del sistema telegráfico francés para obtener información financiera.
- Durante la década de 1970, el delito informático ganó notoriedad con el "phreaking", que consistía en manipular tonos telefónicos para obtener llamadas gratuitas.
- Con la llegada de computadoras y redes, comenzaron a surgir virus y programas maliciosos, siendo el "Creeper" de 1970 el primer virus conocido, seguido por "Reaper", el primer antivirus.
- En los años 80 y 90, con el auge del correo electrónico y los navegadores web, la ciberdelincuencia se diversificó con estafas como el "príncipe nigeriano", virus propagados por la web y el aumento del robo de identidad con la aparición de redes sociales.
- En los 2000 la ciberdelincuencia evolucionó hacia una industria criminal global organizada, con ataques sofisticados como ransomware y fraudes masivos.

Actores y motivos de los Ciberdelincuentes.-

- 1) **Actores estatales:** Son gobiernos que emplean la ciberdelincuencia para **espionaje**, **sabotaje** y operaciones geopolíticas. Buscan obtener ventajas estratégicas, militares y económicas mediante ciberataques dirigidos, como **robos de propiedad intelectual** y **campañas de desinformación**. Ejemplos incluyen grupos vinculados a Rusia, China, Corea del Norte e Irán.
- 2) **Grupos de ciberdelincuencia organizada:** Motivados principalmente por fines económicos, estos grupos altamente profesionales realizan ataques como ransomware, estafas y fraudes masivos. Operan mercados clandestinos y ofrecen servicios criminales en la red, como el alquiler de malware (Ransomware-as-a-Service).
- 3) **Hacktivistas:** Actores que realizan ciberataques con fines ideológicos, políticos o sociales para promover causas específicas. Aunque menos sofisticados que los estados o grupos organizados, han ganado relevancia en conflictos recientes.
- 4) **Insiders o amenazas internas:** Empleados actuales o ex empleados que, por resentimiento, negligencia o daño intencional, comprometen la seguridad de su organización. No siempre tienen la misma sofisticación técnica, pero representan un riesgo importante por su acceso privilegiado.
- 5) **Cibercriminales novatos y oportunistas**: Personas con conocimientos limitados que emplean herramientas sencillas de dominio público para cometer delitos simples en línea.

Bienes jurídicos protegidos:

La legislación contra los delitos informáticos protege varios bienes jurídicos fundamentales, entre los cuales destacan:

- **La integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos**, es decir, que la información contenida en sistemas automatizados se mantenga pura, completa y accesible para sus fines legítimos sin alteraciones no autorizadas.
- **La privacidad y el derecho a la intimidad de las personas**, protegiendo la información personal frente a accesos, usos o divulgaciones ilícitas.
- **El patrimonio**, es decir, los bienes económicos y derechos patrimoniales que pueden ser afectados a través de fraudes, estafas o robos cometidos por medios informáticos.
- **La fe pública y la seguridad en las transacciones** realizadas a través de tecnologías digitales.
- **La protección del correcto funcionamiento de los sistemas de tratamiento de datos**, garantizando que no sean saboteados o vulnerados para impedir sus operaciones legítimas.

Datos sensibles atacados.-

- Los datos y derechos que pueden ser atacados son:

- 1) INFORMACIÓN PERSONAL
- 2) CREDENCIALES DE ACCESO
- 3) INFORMACIÓN FINANCIERA
- 4) DATOS CORPORATIVOS
- 5) DATOS MÉDICOS Y DE SALUD
- 6) COMUNICACIONES PRIVADAS
- 7) INFORMACIÓN EN DISPOSITIVOS CONECTADOS

Datos sensibles atacados.-

- 1) INFORMACIÓN PERSONAL
- Para robo de identidad y fraudes (phishing)
  - 1. Nombres completos
  - 2. Direcciones
  - 3. Fechas de nacimiento
  - 4. Números de identificación
  - 5. Números de teléfonos
  - 6. Correos electrónicos
  - 7) Estados civiles

Datos sensibles atacados.-

- 2) CREDENCIALES DE ACCESO
- Permiten ingresar a sistemas, cuentas bancarias, correos, redes sociales:
  - 1. Nombres de usuarios
  - 2. Contraseñas
  - 3. Token de autenticación
  - 4. Datos biométricos

Datos sensibles atacados.-

3) INFORMACIÓN FINANCIERA

- Para fraude económico:
  - 1. Números de tarjetas de crédito
  - 2. Cuentas bancarias
  - 3. Historiales de transacciones
  - 4. Datos fiscales

Datos sensibles atacados.-

- 4) DATOS CORPORATIVOS
  - 1. Secretos comerciales
  - 2. Propiedad intelectual
  - 3. Información confidencial sobre:
    - Productos
    - Estrategias
    - Clientes
    - Proveedores

Datos sensibles atacados.-

5) DATOS MÉDICOS Y DE SALUD

- Causan daño a la privacidad:
  - 1. Historias clínicas
  - 2. Diagnósticos
  - 3. Tratamientos
  - 4. Seguros

Datos sensibles atacados.-

6) COMUNICACIONES PRIVADAS

Pueden ser usados para chantaje, extorsión:

- 1. Correos electrónicos
- 2. Mensajes
- 3. Grabaciones

Datos sensibles atacados.-

7) INFORMACIÓN EN DISPOSITIVOS CONECTADOS

- 1. Datos de internet
- 2. Datos de cámaras, sensores
- 3. Otros.

El Convenio de Budapest.-

- El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 bajo el amparo del Consejo de Europa y en vigor desde 2004, es el primer tratado internacional para combatir los delitos informáticos

- El Convenio tipifica delitos informáticos como:
  - acceso ilícito,
  - interceptación ilegítima,
  - fraudes,
  - delitos relacionados con contenido de pornografía infantil y
  - violaciones a la propiedad intelectual

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **Artículo 1. Objeto de la Ley**

- **P**revenir y sancionar las conductas ilícitas que
  - afectan los sistemas
  - Afectan a los datos informáticos
  - afectan otros bienes jurídicos de relevancia penal,
    - mediante la utilización de tecnologías de la información o de la comunicación,
      - con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia
    - con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia .

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

La Ley 30096 tipifica:

- Delitos contra datos y sistemas informáticos:
  - Acceso ilícito,
  - Atentado a la integridad de datos y sistemas).
- Delitos informáticos contra la indemnidad y libertad sexuales:
  - Proposiciones sexuales a menores por medios tecnológicos).
  - Grooming
- Delitos informáticos contra la intimidad y el secreto de las comunicaciones.
- Delitos informáticos contra el patrimonio
- Delitos informáticos contra la fe pública.

UNIDAD II:

LOS DELITOS INFORMÁTICOS

Tipos de delitos informáticos clásicos

- **Phishing:** Suplantación de identidad
- **Robo de identidad:** Uso fraudulento de datos personales
- **Ransomware:** Secuestro de datos mediante malware
- **Piratería de software:** Copiar o distribuir software protegido
- **Ciberacoso:** Difusión de información para humillar
- **Abuso infantil:** Uso de medios digitales para acoso o pornografía infantil
- **Fraudes informáticos:** Manipulación de datos o sistemas
- **Ataques DDoS:** interrupción del servicio de páginas web o redes
- **Malware:** software malicioso

Delitos informáticos clásicos

- **Phishing:** Suplantación de identidad
- **Robo de identidad:** Uso fraudulento de datos personales
- **Ransomware:** Secuestro de datos mediante malware
- **Piratería de software:** Copiar o distribuir software protegido
- **Ciberacoso:** Difusión de información para humillar
- **Abuso infantil:** Uso de medios digitales para acoso o pornografía infantil
- **Fraudes informáticos:** Manipulación de datos o sistemas
- **Ataques DDoS:** interrupción del servicio de páginas web o redes
- **Malware:** software malicioso

Delitos: modalidades informáticas

- 1) Acosadores digitales
- 2) APTs digitales (Amenazas Persistentes Avanzadas)
- 3) Bot farms (granjas de cuentas)
- 4) Botnets
- 5) Bots eadores digitales
- 6) Ciberdelincuentes organizados
- 7) Ciberterrorista
- 8) Crackers
- 9) Cyborg delincuentes
- 10) Delicuentes ciberneticos de cuello blanco
- 11) Delincuentes oportunistas
- 12) Gusanistas
- 13) Hacker
- 14) Hackers Black Hat (Sombrero Negro)
- 15) Hackers Blue Hat (sombrero azul)

Delitos: modalidades informáticas

- 16) Hackers éticos (White Hat)
- 17) Hackers Green Hat (sombrero verde)
- 18) Hackers Grey Hat (Sombrero Gris)
- 19) Hackers Red Hat (sombrero rojo)
- 20) Hackers White Hat (Sombrero Blanco)
- 21) Hactivistas
- 22) Hurtadores informáticos
- 23) Insiders o autores internos
- 24) Ladrones informáticos
- 25) Malwaristas
- 26) Pharming
- 27) Phising digitales (pescadores)
- 28) Piratas digitales
- 29) Qrshing

Delitos: modalidades informáticas

- 30) Ransowares (secuestradores digitales)
- 31) Saboteadores digitales
- 32) Script Kiddies
- 33) Sim Swapping
- 34) Smishing
- 35) Sock puppets (Tìteres digitales
- 36) Spear Phishing
- 37) Spyware
- 38) Troyanos
- 39) Viejoverdes digitales (grooming)
- 40) Vihing
- 41) Virus
- 42) Whaling
- 43) Whishing
- 44) Whistleblowers

Tecnologías utilizadas para delinquir

- **Metasploit:** Framework poderoso para pruebas de penetración y explotación de vulnerabilidades en sistemas y redes.
- **Nmap**: Herramienta para escaneo de redes y detección de hosts y puertos abiertos.
- **OpenVAS**: Escáner de vulnerabilidades de red con pruebas conocidas (NVT) para identificar fallas en sistemas.
- **BetterCap**: Utilizada para ataques de hombre en el medio (MITM), interceptación y manipulación en tiempo real de tráfico de red.
- **Armitage**: Interface gráfica para Metasploit que facilita la explotación y administración de sistemas comprometidos.
- OWASP ZAP (Zed Attack Proxy): Plataforma para analizar la seguridad de aplicaciones web y descubrir vulnerabilidades.
- **Herramientas de sniffing** y captura de paquetes para interceptar comunicaciones.
- **Kits de phishing y malware**: Programas para crear campañas de engaño y distribuir software malicioso.
- **Herramientas para escalada de privilegios** y post-explotación como Meterpreter.

DELITOS INFORMÁTICOS CLÁSICOS

Phising

- Suplantación de identidad para obtener datos confidenciales.
- - Datos robados: contraseñas, tarjetas, accesos.
- - Métodos: correos falsos, webs fraudulentas, SMS maliciosos.
- - Consecuencia: pérdidas económicas y robo de identidad.

Suplantación de identidad para engañar a las víctimas y obtener información confidencial. Ejemplo: obtención de contraseñas o datos bancarios.

Phising

- Suplantación de identidad para obtener datos confidenciales.
- - Datos robados: contraseñas, tarjetas, accesos.
- - Métodos: correos falsos, webs fraudulentas, SMS maliciosos.
- - Consecuencia: pérdidas económicas y robo de identidad.

Suplantación de identidad para engañar a las víctimas y obtener información confidencial. Ejemplo: obtención de contraseñas o datos bancarios.

AZ
2025

EL Phising

- Antecedentes: El phishing comenzó a practicarse a mediados de los años 90. El primer incidente ocurrió contra America Online (AOL), la principal proveedora de internet en Estados Unidos en esa época. Ciberdelincuentes se hacían pasar por empleados para engañar a usuarios y solicitar contraseñas bajo pretextos falsos. Posteriormente, los ataques de phishing se extendieron a servicios financieros y plataformas digitales.
- Concepto: Phishing es una técnica de ingeniería social utilizada para engañar a una víctima haciéndose pasar por una entidad confiable, con el fin de obtener información confidencial, como contraseñas, datos bancarios o personales. Se realiza principalmente mediante correos electrónicos, mensajes o páginas web falsas que inducen a la víctima a revelar datos sensibles o descargar malware. El término "phishing" deriva del verbo inglés "fishing" (pescar), haciendo referencia a "pescar" víctimas con un cebo.

AZ
2025

EL Phising

- Casos recientes relevantes:
- En 2023, el Sistema de Salud Hospital Sisters sufrió un ciberataque que comprometió datos personales de 882,000 pacientes, logrados a través de técnicas de phishing.
- En 2023, MGM Resorts International fue víctima de un ataque que incluyó suplantación de identidad por voz y accesos indebidos.
- En 2025, la empresa Finastra informó de una brecha de datos tras acceso ilícito a su plataforma segura.
- En 2025, la tienda online de Casio UK fue atacada con scripts maliciosos que robaron datos de tarjetas de crédito y clientes.
  Estas muestra la gran variedad de sectores afectados por phishing, desde salud hasta comercio electrónico, con pérdidas millonarias y exposición de datos sensibles.

AZ
2025

EL Robo de identidad como delito informático:

Robo de Identidad

- Uso fraudulento de datos personales.
- - Ejemplos: abrir cuentas, solicitar créditos, compras online.
- - Impacto: problemas legales, daños financieros y reputacionales.

Uso fraudulento de datos personales para acceder a recursos o cometer fraudes.

AZ
2025

EL Robo de identidad como delito informático:

- Antecedentes: El robo de identidad como delito informático tiene sus orígenes en el incremento del uso de tecnologías digitales, donde la obtención y uso no autorizado de datos personales empezó a ser un método para cometer fraudes y otros delitos. En la legislación peruana y muchas otras, inicialmente se contemplaba como una agravante dentro de otros delitos hasta que se tipificó de forma autónoma para abordar la suplantación de identidad en el entorno digital y la protección de datos.
- Concepto: El robo de identidad es la acción ilegal de apropiarse de los datos personales de otra persona —como nombre, números de cuentas bancarias, documentos oficiales y contraseñas— para suplantar su identidad y realizar actividades fraudulentas, como contratar servicios, acceder a recursos o realizar operaciones financieras en nombre de la víctima. Es considerado un delito informático porque se perpetra mediante el acceso no autorizado a información digital o sistemas informáticos. Puede implicar desde la suplantación en redes sociales hasta usos ilegítimos en ámbitos legales y económicos.

AZ
2025

EL Robo de identidad como delito informático:

- Casos relevantes:
- En Estados Unidos en 2021 se estimaron pérdidas de miles de millones de dólares debido al robo de identidad y fraudes asociados, con millones de víctimas reportadas.
- En 2023, investigaciones detectaron bandas criminales que robaban identidades para crear documentos falsos o realizar fraudes financieros.
- En América Latina, se reportaron casos de suplantación en redes sociales usadas para estafar a usuarios y obtener beneficios ilícitos.
- En Perú, las autoridades han intervenido bandas dedicadas a la suplantación de identidad telefónica y digital con multas y penas de prisión.
- Casos mediáticos incluyen la venta de datos personales robados y la suplantación para realizar compras o cometer otros ciberdelitos.

AZ
2025

EL Ransomware:

.

Ransomware

- Secuestro de datos mediante malware.
- Funciona cifrando archivos y exigiendo pago.
- Consecuencias: pérdida de datos, paralización de servicios, sin garantía de devolución.

Secuestro de datos mediante malware que bloquea el acceso hasta que se pague un rescate.

AZ
2025

EL Ransomware:

- Antecedentes: El primer ataque documentado de ransomware ocurrió en 1989 con el llamado "Troyano del SIDA" o "PC Cyborg". El biólogo Joseph L. Popp envió 20,000 disquetes infectados a participantes de una conferencia sobre el SIDA, los cuales cifraban los archivos después de varios reinicios y pedían un rescate de 189 dólares para proporcionar la clave de descifrado. Este método fue primitivo, ya que el pago se hacía por correo postal y fue rastreado hasta Panamá. Después, el ransomware permaneció poco visible hasta la evolución de las criptomonedas que facilitaron pagos difíciles de rastrear, creando un auge de ataques a partir de 2010-2011, con CryptoLocker y WannaCry como casos emblemáticos.

AZ
2025

EL Ransomware:

- Concepto:
  El ransomware es un tipo de malware que cifra los archivos o bloquea el acceso a sistemas completos y luego exige un pago (rescate) para devolver el acceso al usuario legítimo. Esto interrumpe la operación normal de individuos o empresas, causando pérdidas económicas y daños operativos significativos. Sus métodos incluyen phishing para propagar el malware, y métodos de pago anónimos como bitcoins para evitar rastreo.

AZ
2025

EL Ransomware:

- Casos destacados:
- WannaCry (2017): afectó a más de 200,000 computadoras en 150 países, incluyendo hospitales y grandes corporaciones.
- NotPetya (2017): ataque dirigido a Ucrania que se propagó globalmente, causando pérdidas millonarias.
- Ataques recientes (2024-2025) a grandes compañías como Acer, Brenntag y Finastra, que sufrieron interrupciones y robo de datos por ransomware.
- El ransomware es actualmente una de las mayores amenazas cibernéticas, con constantes evoluciones técnicas y estratégicas por parte de los atacantes, haciendo necesaria la preparación y medidas proactivas de ciberseguridad.
- El ransomware es un delito que va desde ataques rudimentarios a sofisticados ataques globales modernos solicitando rescates en criptomonedas.

AZ
2025

La Piratería de Soffware:

.

Piratería de Software

- Copia o distribución ilegal de programas.
- Formas: descargas piratas, compartir licencias.
- Riesgos: sanciones legales, malware oculto, pérdida de soporte.

Copia o distribución ilegal de programas protegidos por derechos de autor.

AZ
2025

La Piratería de Soffware:

- Antecedentes: La piratería de software comenzó a tomar relevancia en las décadas de 1970 y 1980, cuando el software empezó a considerarse un producto valioso con derechos de autor protegidos. Inicialmente, la copia no autorizada de programas de computadora se realizaba sin consecuencias legales claras, ya que la protección legal del software era limitada. La transformación más significativa ocurrió cuando compañías como Microsoft, impulsadas por Bill Gates, defendieron los derechos de autor sobre el software, llevando a leyes y regulaciones para proteger la propiedad intelectual de estas obras digitales. Antes de la expansión de Internet, la distribución ilegal de software se realizaba a través de sistemas de tablones de anuncios (BBS) con conexiones dial-up, donde usuarios compartían programas ilegalmente. La llegada de Internet y luego las redes punto a punto (P2P) facilitaron un acceso masivo y descentralizado al software pirata, complicando su control legal y técnico.

AZ
2025

La Piratería de Soffware:

- Concepto:
  La piratería de software es la copia, distribución, venta o uso ilegal de programas informáticos sin la licencia correspondiente. Esto incluye desde la duplicación de software comercial sin permiso hasta la distribución masiva de copias ilegales por medios digitales. Además de la violación de derechos de autor, afecta negativamente a las empresas desarrolladoras por la pérdida de ingresos y puede representar riesgos de seguridad para los usuarios debido a versiones modificadas o dañinas del software. La piratería va desde el uso personal no autorizado hasta operaciones comerciales ilícitas en gran escala.

AZ
2025

La Piratería de Soffware:

- Casos relevantes:
- Durante los años 90 y 2000, la piratería masiva a través de discos piratas fue crítica en varios países, afectando la industria informática mundial.
- En la actualidad, la piratería digital continúa siendo un problema global, con miles de millones de dólares en pérdidas anuales para la industria del software.
- Casos en la industria del entretenimiento y software educativo han exhibido ventas masivas de productos ilegales en mercados locales e internacionales.
- Interpol y otras agencias internacionales continúan operativos contra redes de distribución de software pirata principalmente en Asia y América Latina.
- Empresas líderes han impulsado campañas de concientización y tecnologías DRM (gestión de derechos digitales) para proteger sus productos.

AZ
2025

El Ciberacoso:

.

Ciberacoso

- Difusión de información dañina para humillar.
- Modalidades: insultos, rumores, difusión de imágenes privadas.
- Consecuencias: daño reputacional, ansiedad, depresión.

Difusión de información dañina para humillar o afectar psicológicamente a una persona.

AZ
2025

El Ciberacoso:

- Antecedentes:
  El ciberacoso surge como una extensión del acoso tradicional o bullying que ocurre en plataformas digitales con el crecimiento del internet y las redes sociales. Sus orígenes están vinculados al bullying escolar reportado desde la década de 1970-1980 en países nórdicos, donde se diferenciaba entre acoso físico y psicológico. Con el auge del internet, especialmente a partir de 2000 y la masificación de redes sociales, el acoso migró a espacios digitales ampliando su alcance y complejidad. Este fenómeno viralizó casos de acoso virtual con consecuencias sociales y legales, siendo un problema creciente y aún en estudio y prevención.

AZ
2025

El Ciberacoso:

- Concepto:
  El ciberacoso o cyberbullying se define como la intimidación o agresión intencional y repetida realizada a través de medios electrónicos, como mensajes, redes sociales o correos electrónicos, hacia una persona con un desequilibrio de poder digital. Se caracteriza por poder ocurrir en cualquier momento y lugar (24/7), a menudo con el anonimato del agresor o mediante la suplantación de identidad, lo que agrava su impacto emocional y social. El ciberacoso puede incluir insultos, amenazas, difusión de rumores, publicación de información o imágenes privadas sin consentimiento, exclusión social digital, entre otras conductas dañinas.

AZ
2025

El Ciberacoso:

- Casos relevantes:
- El caso más emblemático fue el de Amanda Todd, una joven canadiense que sufrió sextorsión y ciberacoso a través de videos íntimos difundidos, que la llevaron al suicidio en 2012, generando campañas globales contra el ciberacoso.
- En 2016, casos en países como México y España han mostrado impactos psicológicos severos en víctimas adolescentes sometidas a bullying y ciberacoso escolar.
- En 2025, la proliferación de casos en plataformas sociales y aplicaciones de mensajería han llevado a la implementación de leyes y campañas de prevención para adultos y jóvenes.
- Las escuelas, familias y autoridades incrementan programas educativos para mitigar el ciberacoso y ofrecer apoyo a las víctimas.

AZ
2025

El delito informático de abuso infantil:

.

Abuso Infantil

- Uso de medios digitales para explotación de menores.
- Formas: grooming, pornografía infantil.
- Gravedad: delito severamente penado, consecuencias irreversibles.

Uso de tecnología para la explotación o acoso sexual menores.

AZ
2025

El delito informático de abuso infantil:

- Antecedentes:
  El delito de abuso infantil en el entorno informático emergió con el avance de las tecnologías y el Internet, que facilitaron nuevas formas de explotación y abuso sexual de menores a través de medios digitales. Conceptos como el "child grooming" o acoso sexual en línea, donde un adulto contacta y manipula a menores para obtener material o encuentros sexuales, se reconocieron formalmente en legislación reciente. En Perú, por ejemplo, el delito está tipificado en la Ley N° 30096 desde 2013 y ha sufrido modificaciones para adaptarse a las nuevas formas de criminalidad en línea, considerando la gran vulnerabilidad de niños y adolescentes ante estos delitos.

AZ
2025

El delito informático de abuso infantil:

- Concepto:
  El delito informático de abuso infantil involucra el uso de tecnologías como internet, redes sociales, aplicaciones de mensajería y otras plataformas digitales, para contactar, manipular o coaccionar a menores con fines sexuales o para obtener material pornográfico infantil. Incluye la creación de perfiles falsos para ganarse la confianza del menor, obligarlo a enviar imágenes o videos íntimos o incluso concertar encuentros físicos que conlleven al abuso. Se protege en legislación penal el bien jurídico de la libertad e indemnidad sexual de niños, niñas y adolescentes, tipificándose como delito de proposiciones a menores por medios tecnológicos sin necesidad de que el acto sexual haya ocurrido, siendo suficiente la intención.

AZ
2025

El delito informático de abuso infantil:

- Casos relevantes:
- El fenómeno del grooming ha sido detectado en diversas redes sociales famosas como Facebook, WhatsApp, Instagram, TikTok, con múltiples denuncias que involucran a adultos ocultos detrás de perfiles falsos.
- En Perú y otros países latinoamericanos, hubo sentencias contra personas que contactaban a menores para solicitar material pornográfico o encuentros sexuales a través de medios electrónicos.
- Casos mediáticos a nivel mundial, similares al caso de Amanda Todd
- Las autoridades judiciales y policiales vienen fortaleciendo unidades especializadas para investigar y sancionar estos delitos, con penas que pueden ir desde 3 a 9 años de prisión efectiva según la gravedad y modalidad de la infracción.
- El delito informático de abuso infantil es una grave violación a la integridad y libertad sexual de los menores utilizando tecnologías digitales, con un componentes específicos de manipulación y coerción virtual

AZ
2025

El delito informático de abuso infantil: el GROOMING

- El grooming es un delito que se refiere al acercamiento gradual y engañoso de un adulto hacia un menor a través de medios digitales, con la finalidad de obtener beneficios sexuales o materiales, como imágenes o videos íntimos del menor, o concertar encuentros físicos para abusar de él.
- Concepto: El groomer (adulto) contacta al menor por internet, teléfono u otro medio digital, ganándose su confianza con engaños, fingiendo amistad o cercanía.
- El proceso suele incluir solicitudes para enviar material pornográfico o concertar encuentros personales con fines sexuales.
- La legislación tipifica el grooming como un delito contra la libertad e indemnidad sexual de menores, con penas de prisión y multas. Por ejemplo, en España está regulado en el artículo 183 ter del Código Penal.

AZ
2025

El delito informático de abuso infantil: el GROOMING

- Las penas varían según intentos de concierto de encuentro o solicitud de material pornográfico, pudiendo ir desde seis meses a tres años, y mayores si se usan coacciones o intimidación.
- Además, este delito vulnera derechos fundamentales como la intimidad, la propia imagen, la libertad sexual y la seguridad digital del menor.

AZ
2025

El delito informático de abuso infantil: el GROOMING

- Antecedentes:
- La tipificación del grooming se ha dado a partir de la expansión de internet y redes sociales, en respuesta a la creciente explotación digital de menores.
- La legislación internacional, como la Convención de los Derechos del Niño y directivas europeas, impulsan las regulaciones nacionales para proteger a los menores de estas nuevas formas de abuso digital.

AZ
2025

El delito informático de abuso infantil: el GROOMING

- Casos:
- Casos emblemáticos como el de Amanda Todd evidencian el impacto psicológico y social del grooming.
- En Perú, la Ley N° 30096 tipifica proposiciones a menores con fines sexuales por medios tecnológicos, con penas de prisión considerables.
- Autoridades judiciales han condenado a personas dedicadas al grooming, incluyendo quienes amenazan o chantajean a menores con difusión de material íntimo para obtener más.
- Las investigaciones sugieren que el grooming es un método frecuente en redes sociales populares y apps de mensajería, con esfuerzos institucionales para su prevención.

AZ
2025

El Fraude informático:

.

Fraudes Informáticos

- Manipulación de datos o sistemas con fines económicos.
- Ejemplos: modificaciones bancarias, estafas en comercio electrónico.
- Consecuencias: pérdidas millonarias, desconfianza digital.

Manipulación de datos o sistemas para beneficio económico ilícito.

AZ
2025

El Fraude informático (engañar para sustraer):

DEFINICIONES:

- El fraude informático es un delito que consiste en utilizar medios informáticos o digitales para engañar a una persona o entidad con el fin de obtener un beneficio ilícito, generalmente económico. Implica acciones deliberadas para manipular información, suplantar identidades, acceder sin autorización a sistemas o datos, y engañar a las víctimas para sustraer dinero, información confidencial o realizar transacciones fraudulentas.

- El fraude informático es una forma de delincuencia que utiliza el engaño y la manipulación tecnológica para obtener beneficios ilegítimos, afectando tanto a personas como a organizaciones en el ámbito digital y financiero.

AZ
2025

El Fraude informático (engañar para sustraer):

DEFINICIÓN LEGAL – LEY DE DELITOS INFORMÁTICOS – LEY 30096.-

- **Artículo 8. Fraude informático**

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos."

AZ
2025

El Fraude informático (engañar para sustraer):

CARACTERÍSTICAS:

- El fraude informático se caracteriza por:
  - 1) El uso de sistemas informáticos para manipular datos o información.
  - 2) La acción deliberada e ilegítima, con intención de obtener un provecho ilícito.
  - 3) El perjuicio causado a otra persona o entidad.
  - 4) Puede incluir la alteración, borrado, supresión, clonación de datos o cualquier interferencia en sistemas informáticos.

AZ
2025

TIPOS de Fraude informático (engañar para sustraer):

TIPOS DE FRAUDES INFORMÁTICOS

- 1) Phishing (robo y suplantación de identidad para obtener datos bancarios, credenciales):
- 2) Vishing (llamada fraudulenta)
- 3) Smishing: (mensaje fraudulento)
- 4) Ransomware: (software malicioso para robar o bloquear información)
- 5) Carding: (Uso fraudulento de tarjetas de crédito robadas)
- 6) Acceso no autorizado
- 7) Fraude en comercio electrónico: sitios falsos que no entregan productos.
- 8) Manipulación de transferencias electrónicas para desviar fondos.

AZ
2025

TIPOS de Fraude informático:

Tipos comunes de fraudes informáticos incluyen:

- **1.- Phishing:** Suplantación de identidad mediante correos electrónicos, mensajes o sitios web falsos para obtener datos sensibles como contraseñas o números de tarjetas de crédito.

- **2.- Vishing: C**onsiste en llamadas telefónicas fraudulentas que buscan obtener información personal o bancaria.

- **3.- Smishing:** Utiliza mensajes de texto o WhatsApp para engañar a la víctima y obtener datos confidenciales.

- **4.- Suplantación de identidad:**
  - Robo de datos personales para realizar operaciones fraudulentas o acceder a cuentas digitales ajenas.

AZ
2025

El Fraude informático:

- Tipos comunes de fraudes informáticos incluyen:
- **5.-Ransomware:**
  - Malware que bloquea o cifra los datos de un sistema y exige un rescate para liberar el acceso.
- **6.- Carding:**
  - Uso ilegal de datos de tarjetas de crédito robadas para realizar compras o transacciones.
- **7.- Acceso no autorizado:**
  - Intrusión en sistemas informáticos para modificar, robar información o causar daños.

AZ
2025

El Fraude informático:

- Antecedentes:
- Los fraudes informáticos tienen antecedentes que se remontan a la evolución de las tecnologías de la información y comunicación desde mediados del siglo XX. Los primeros delitos informáticos se reportaron en la década de los 70 y 80, vinculados a actividades de espionaje, sabotaje y uso indebido de sistemas informáticos. Un ejemplo temprano fue el uso de dispositivos como la "caja azul" para realizar llamadas telefónicas gratuitas ilícitas. A medida que Internet se masificó en los años 90 y 2000, también crecieron los métodos de fraude, como el robo de identidad, phishing y ataques con software malicioso para obtener ganancias ilícitas.

AZ
2025

El Fraude informático:

Concepto: El fraude informático es un delito que

- Consiste en engañar o manipular a personas, sistemas o entidades
- A través de medios electrónicos
- Para obtener un beneficio ilícito, generalmente económico.
- Involucra:
  - Manipulación de información,
  - Suplantación de identidades,
  - Acceso no autorizado,
  - y otros mecanismos tecnológicos para defraudar.

Este delito es una modalidad de fraude adaptada al entorno digital, con mecanismos complejos que incluyen ataques dirigidos a bancos, usuarios individuales y empresas, socavando la confianza en el comercio electrónico y los sistemas digitales.

AZ
2025

El Fraude informático:

- Casos relevantes:
- El caso del gusano Morris en 1988, que aunque fue un experimento, causó daños masivos y representó una señal de la vulnerabilidad creciente de las redes.
- Fraudes multimillonarios por medio de phishing, vishing y smishing en el sector bancario y financiero globalmente.
- Robos masivos de datos personales usados para fraudes en tarjetas de crédito y creación de identidades falsas.
- Ataques ransomware que, además de extorsionar, roban datos y causan parálisis en instituciones.
- Casos recientes en 2024 y 2025 reflejan ataques coordinados a empresas tecnológicas, bancos y servicios críticos que han provocado pérdidas económicas significativas y robos de información sensible.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

- Los fraudes informáticos mediante páginas clonadas falsas, también conocidos como phishing, son una de las modalidades de ciberdelincuencia más denunciadas en Perú en 2025. Consisten en la creación de sitios web que imitan con alta fidelidad a páginas oficiales, como las de entidades bancarias, con el fin de engañar a los usuarios y obtener sus datos personales y financieros, como número de DNI, claves, números de tarjeta y otros datos sensibles.

- Estas páginas falsas inducen a la víctima a ingresar sus datos bajo pretextos engañosos, como actualizar información o participar en promociones, lo que permite a los delincuentes acceder a cuentas bancarias y realizar fraudes económicos. El phishing puede complementarse con técnicas como el vishing (phishing vía llamadas telefónicas con voz suplantada) y otras formas de suplantación de identidad.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

- **Herramientas gratuitas para verificar si una web es legítima:**

Para verificar si una web es legítima, se pueden usar diversas herramientas gratuitas que analizan aspectos técnicos, reputación y seguridad del sitio:

- 1) VirusTotal: Escanea URL en busca de malware y phishing usando varios motores antivirus y listas negras. Ofrece informes detallados y reputación comunitaria.
- 2) Whois (ICANN): Permite conocer datos de registro del dominio, como fecha de creación, propietario y servidores de nombres, útil para identificar sitios creados recientemente o con datos ocultos.
- 3) Google Transparency Report: Informa sobre la seguridad de un sitio y si ha sido reportado como peligroso o inseguro.
- 4) Talos Intelligence: Proporciona análisis de reputación de dominios y comprobación contra listas negras.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

Herramientas gratuitas para verificar si una web es legítima:

- 5) Kaspersky VirusDesk: Escanea y reporta si un sitio tiene malware o es malicioso, además de la reputación del dominio.
- 6) URLVoid: Evalúa el sitio con más de 30 motores antivirus para detectar amenazas y listar detalles del dominio.
- 7) Sucuri SiteCheck: Escáner gratuito que detecta malware, errores y códigos maliciosos en sitios web.
- 8) PhishTank: Base de datos colaborativa para identificar sitios de phishing.
- 9) Desenmascara.me: Herramienta española que analiza sitios y otorga una puntuación de seguridad considerando diversos parámetros técnicos y reputacionales.
- 10) Scamadviser: Ofrece un análisis sencillo de riesgo y reputación de sitios web, con detalles del propietario y calidad del dominio.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

PLANTILLA DE INFORME PERICIAL: Una plantilla de informe pericial para clonación de sitio web debe incluir las siguientes secciones esenciales, adaptables según la naturaleza del caso:

- **1) Identificación del Perito: Nombre completo, DNI, título profesional, número de colegiado, experiencia y datos de contacto.**
- **2) Juramento o declaración de veracidad: Compromiso del perito de decir la verdad y actuar con objetividad.**
- **3) Objeto del informe: Descripción clara del propósito del peritaje, en este caso, demostrar la clonación de un sitio web.**
- **4) Antecedentes y solicitud: Datos sobre la solicitud del informe, partes involucradas y contexto del caso.**
- **5) Marco normativo: Legislación y normativa aplicable al delito o caso pericial.**

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

PLANTILLA DE INFORME PERICIAL:

- 6) Metodología aplicada: Técnicas y herramientas usadas para obtener, comparar y analizar el código HTML, recursos y estructuras de ambos sitios (original y supuesto clon).
- 7) Cadena de custodia: Detalle del proceso de preservación y manejo de la evidencia digital para asegurar su integridad.
- 8) Análisis de pruebas: Descripción detallada con evidencias técnicas, comparativas de texto, recursos, URLs, firmas digitales, etc., que demuestran la clonación.
- 9) Resultados y hallazgos: Conclusiones claras, basadas en la evidencia, señalando la existencia de clonación y posibles manipulaciones.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

PLANTILLA DE INFORME PERICIAL:

- 10) Conclusión: Síntesis final del dictamen técnico, indicando si el sitio web ha sido clonado conforme a la evidencia.
- 11) Anexos: Documentación adicional, capturas de pantalla, tablas comparativas, informes de herramientas utilizadas.
- 12) Firma y certificación del perito.

- Este modelo debe seguir normas y estándares forenses para garantizar la admisibilidad judicial, como la Norma UNE 157001:2002. El informe debe ser claro, objetivo, técnico, pero comprensible para personas no expertas.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- **INFORME PERICIAL INFORMÁTICO**
- **Perito: [Nombre Completo]**
- **Colegiatura: [Número y Colegio Profesional]**
- **Fecha: [Fecha del informe]**
- **Caso: Phishing por clonación de sitio web**

- **1. Objeto del informe**
- **El presente informe tiene por objeto determinar la existencia de clonación del sitio web [URL original] con la finalidad de realizar actividades fraudulentas (phishing) dirigidas a obtener datos personales de usuarios.**

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- **2. Antecedentes.- Se recibió solicitud de peritaje ante la denuncia presentada por [Nombre denunciante/empresa], debido a reportes de usuarios que fueron redirigidos a un sitio falso que imitaba al sitio oficial.**
- **3. Marco normativo.- Ley N° 30096 - Ley de Delitos Informáticos (Artículo 8 - Fraude Informático). Normativas internacionales a criterio.**
- **4. Metodología.- Recolección de URLs y muestras del sitio original y presuntamente clonado.**
- **Análisis comparativo de código HTML, recursos multimedia y estructura del sitio mediante herramientas [indicar herramientas].**
- **Identificación de diferencias y elementos fraudulentos mediante comparación visual y técnica.**

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- **Verificación de certificado SSL y datos de registro WHOIS del dominio falso.**
- **Documentación fotográfica de capturas de pantalla y hashes para cadena de custodia.**

- **5. Análisis de pruebas.-**
  - La URL del sitio clonado ([URL falsa]) presenta caracteres adicionales y diferente dominio que imita el oficial.
  - El código HTML y recursos multimedia son una copia casi exacta del sitio oficial, con modificaciones en los formularios de autenticación para capturar datos.
  - Falta certificación SSL válida en el sitio falso, mostrando advertencias en navegadores.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- Registro WHOIS del dominio falso indica fecha de creación reciente y propietario desconocido.
- Capturas de pantalla demuestran similitud visual, pero con enlaces redirigidos a servidores distintos.
- Se detectaron scripts insertados para envío automático de datos a terceros no autorizados.

- **6. Resultados y conclusiones**
  - Se concluye que el sitio web [URL falsa] es un clon malicioso del sitio oficial [URL original], creado con propósito fraudulento de phishing para obtener credenciales y datos personales de los usuarios.
  - Se recomienda tomar las medidas legales correspondientes y alertar a usuarios y proveedores de dominio y hosting para su cierre.

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- **7. Anexos**
  - Capturas de pantalla comparativas.
  - Reportes técnicos de herramientas de comparación.
  - Reportes WHOIS y certificados SSL.
  - Documentación de cadena de custodia.

- **Firma:**
- **[Nombre y firma del perito]**
- **[Certificaciones]**

AZ
2025

El Fraude informático. PÁGINAS CLONADAS FALSAS:

MODELO DE INFORME PERICIAL DE WEB CLONADA:

- **EL REGISTRO WHOIS** es un directorio público de Internet que contiene información sobre los propietarios de nombres de dominio y direcciones IP. Permite saber quién es el propietario de un dominio, cuándo se registró, cuándo caduca y qué servidores de nombres utiliza. Por motivos de privacidad, especialmente debido al RGPD, la información de contacto de los propietarios (como nombre, dirección y teléfono) suele estar oculta en los registros actuales.
- **UN CERTIFICADO SSL** (Secure Sockets Layer) es un pequeño archivo de datos que vincula la identidad de un sitio web con una clave criptográfica, permitiendo una conexión encriptada y segura entre el servidor y el navegador del usuario. Esto se verifica a través del protocolo HTTPS, habilitando el candado en el navegador y protegiendo la información sensible, como datos personales y de pago, de ser interceptada.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- Las compras fraudulentas digitales son un tipo de estafa que ocurre cuando delincuentes utilizan métodos tecnológicos para obtener productos, servicios o dinero de manera ilícita a través de plataformas digitales. Este tipo de fraude puede involucrar el uso de datos robados, como tarjetas de crédito clonadas o cuentas hackeadas, o la manipulación de sitios web mediante técnicas como el phishing y la clonación de páginas para engañar a los usuarios y obtener sus datos financieros.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

CARACTERÍSTICAS DE COMPRAS FRAUDULENTAS DIGITALES:

- Uso de tarjetas de crédito o débito robadas para hacer compras en línea sin el consentimiento del titular.
- Creación de sitios web falsos (clonación) que imitan tiendas legítimas, donde se capturan datos de pago de los usuarios.
- Envío de correos o mensajes fraudulentos que inducen a la víctima a ingresar datos bancarios o información personal en páginas falsas (phishing de clonación).
- Manipulación o interceptación de pagos en plataformas electrónicas para desviar fondos.
- Compra y reventa de productos adquiridos fraudulentamente, afectando a tiendas y consumidores.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

RIESGOS Y CONSECUENCIAS:

- Pérdidas económicas para consumidores y comerciantes.
- Dificultades legales y administrativas para recuperar fondos.
- Deterioro de la confianza en comercio electrónico y plataformas digitales.
- Posibles sanciones legales para las personas involucradas en estos fraudes.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **MEDIDAS DE PREVENCIÓN:**
- Verificar la legitimidad de las páginas web y correos electrónicos antes de introducir datos personales.
- Utilizar métodos de pago seguros que ofrezcan protección ante fraudes.
- Monitorizar transacciones bancarias regularmente para detectar operaciones no autorizadas.
- Implementar sistemas de autenticación fuerte en plataformas digitales.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **CHECKLIST DE LOGS Y METADATOS** imprescindibles para la pericia en compras fraudulentas digitales

- Un "checklist" de logs y metadatos es una lista de verificación que se utiliza para comprobar que los **registros (logs)** y los **datos descriptivos (metadatos)** de un sistema se recopilan, almacenan y gestionan correctamente. Este tipo de checklist asegura que se cumplen los estándares, se minimizan los errores y se obtiene la información necesaria para un análisis posterior de manera sistemática.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **CHECKLIST DE LOGS Y METADATOS** imprescindibles para la pericia en compras fraudulentas digitales

Para un procedimiento pericial informático, especialmente en casos de fraudes digitales como compras fraudulentas o clonación de sitios, una checklist de logs y metadatos imprescindibles debe incluir:

- 1) Logs de acceso y autenticación: Fechas, horas, direcciones IP, nombres de usuario, resultados de autenticación (éxito o fallo), métodos de acceso.
- 2) Registros de transacciones: Detalles completos de las operaciones realizadas, incluyendo montos, cuentas involucradas, timestamps.
- 3) Metadatos de archivos: Información sobre creación, modificación o acceso a documentos digitales o recursos relacionados, incluyendo identificadores únicos (hashes).

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **CHECKLIST DE LOGS Y METADATOS** imprescindibles para la pericia en compras fraudulentas digitales

- 4) Registros del servidor web: Solicitudes HTTP, urls solicitadas, códigos de respuesta, agente de usuario (user-agent), referencias de origen.
- 5) Logs de base de datos: Cambios, consultas, accesos a datos relevantes para la operación sospechosa.
- 6) Metadatos de correos electrónicos: Remitentes, destinatarios, timestamps, IPs originarias, rutas de entrega.
- 7) Datos de red: Capturas de tráfico (pcaps), conexiones establecidas, protocolos usados.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **CHECKLIST DE LOGS Y METADATOS** imprescindibles para la pericia en compras fraudulentas digitales
- 8) Sistema y logs de dispositivos: Registros de sistema operativo, programas antivirus o de seguridad, logs de aplicaciones.
- 9) Información de certificados digitales y SSL: Vigencia, emisores, correspondencia con URLs.
- 10) Registro de acciones del usuario: Clicks, formularios enviados, movimientos del cursor cuando sea posible.
- 11) Cadena de custodia documental: Documentar cómo y cuándo se obtuvieron los logs y metadatos, para garantizar su integridad y validez legal.

AZ
2025

El Fraude informático. COMPRAS FRAUDULENTAS digitales.-

- **CHECKLIST DE LOGS Y METADATOS** imprescindibles para la pericia en compras fraudulentas digitales

Estos datos, tratados con herramientas forenses como Autopsy, FTK, EnCase, o X-Ways, permitirán reconstruir hechos, validar autenticidad y detectar manipulaciones o accesos ilegítimos, asegurando la calidad técnica y jurídica de la prueba pericial.

- La correcta recolección, preservación y análisis de estos logs y metadatos es fundamental para demostrar la mecánica del fraude digital y sustentar procesos judiciales. Esta checklist debe adaptarse según el tipo de fraude y sistema involucrado, pero cubre los elementos críticos que permite un examen completo y fiable.

AZ
2025

El Fraude informático. FALSAS OFERTAS ONLINE.-

- Las falsas ofertas online son una modalidad frecuente de fraude digital que consiste en la creación de tiendas o anuncios falsos que prometen productos con precios muy bajos o promociones irresistibles para atraer a compradores desprevenidos. Estas estafas se caracterizan por imitar la estética y funcionalidades de tiendas legítimas o plataformas populares para engañar a los usuarios y así obtener sus datos personales, bancarios o el pago sin entregar el producto.

AZ
2025

El Fraude informático. FALSAS OFERTAS ONLINE.-

- **CARACTERÍSTICAS DE LAS FALSAS OFERTAS ONLINE:**
- Promesas de descuentos, regalos o productos exclusivos por tiempo limitado.
- URLs falsas que imitan sitios reales, algunas con certificado SSL para aparentar legitimidad.
- Información de contacto faltante o genérica (correos gratuitos, ausencia de dirección o teléfono).
- Pedidos con pago adelantado, usualmente fuera de la plataforma oficial, vía métodos no seguros.
- Imágenes y descripciones robadas o copiadas de sitios legítimos.
- Opiniones o reseñas falsas para generar confianza.

AZ
2025

El Fraude informático. FALSAS OFERTAS ONLINE.-

- **RIESGOS Y CONSECUENCIAS:**
- Pérdida de dinero sin recibir producto alguno.
- Robo de datos personales y bancarios con uso posterior para fraudes.
- Posible usurpación de identidad y apertura de créditos o compras no autorizadas.
- Dificultades para reclamar o recuperar fondos.

AZ
2025

El Fraude informático. FALSAS OFERTAS ONLINE.-

MEDIDAS PARA EVITAR CAER EN ESTAS ESTAFAS:

- Desconfiar de precios demasiado bajos o promociones poco realistas.
- Verificar cuidadosamente la URL y su correspondencia con la página oficial.
- Investigar opiniones reales y experiencias de otros compradores.
- Evitar realizar pagos fuera de la plataforma segura, especialmente por transferencias directas o giros.
- Utilizar extensiones o servicios de seguridad que alerten sobre sitios inseguros.
- Confirmar que exista información clara y verificable de contacto y políticas de devolución.
- La Policía Cibernética y especialistas en ciberseguridad advierten sobre el aumento de estos fraudes, en los que se combinan técnicas de phishing, clonación de páginas y promociones falsas para engaña

Ataques DDoS

- Interrupción de servicios mediante ataques masivos.
- Funcionamiento: miles de dispositivos colapsan servidores.
- Impacto: inaccesibilidad, pérdidas económicas y reputacionales.

Interrupción del servicio de páginas web o redes mediante ataques masivos.

AZ
2025

Los Ataques DDoS

- Antecedentes:
- El primer ataque DDoS documentado ocurrió el 22 de julio de 1999 cuando la Universidad de Minnesota fue atacada por 114 redes infectadas con un malware llamado Trin00, que saturaba el sistema con paquetes de datos inútiles, dejándola fuera de servicio por dos días. Este ataque fue el inicio de una era de ataques de denegación de servicio distribuida. Más tarde, en el año 2000, un joven hacker llamado "Mafiaboy" realizó ataques masivos contra sitios como CNN, Amazon, eBay y Yahoo!, generando caos generalizado. En 2007, una serie de ataques DDoS masivos afectaron a Estonia, considerados como uno de los primeros actos de ciberguerra moderna, relacionados con un conflicto político con Rusia.

AZ
2025

Los Ataques DDoS

- Concepto:
  Un ataque DDoS (Distributed Denial of Service) busca saturar la capacidad de un servidor, red o servicio con una avalancha de tráfico proveniente de múltiples fuentes (botnets), impidiendo el acceso legítimo de usuarios. El objetivo es dejar el sistema inaccesible por sobrecarga, afectando la disponibilidad y continuidad de servicios online, afectando empresas, instituciones gubernamentales e infraestructura crítica. Se ha convertido en una herramienta común y efectiva para ciberdelincuentes, hacktivistas y actores estatales en conflictos cibernéticos.

AZ
2025

Los Ataques DDoS

- Casos relevantes:
- Estonia (2007): Ciberataque masivo dirigido a servicios gubernamentales y bancos, considerado el primer evento de guerra cibernética a gran escala.
- Dyn (2016): Ataque que afectó servicios populares como Twitter, Netflix y Reddit a través de una botnet de dispositivos IoT inseguros.
- GitHub (2018): Sufrió uno de los mayores ataques DDoS conocidos con un tráfico de 1,35 terabits por segundo, que fue mitigado rápidamente.
- Bancos estadounidenses (2012): Se enfrentaron a ataques prolongados de más de 60 gigabits por segundo que ralentizaron sus sistemas por varios días.
- PlayStation Network y Xbox Live (2014): Dejó inoperativos los servicios en línea durante días, afectando a millones de usuarios.
  Estos casos demuestran la capacidad disruptiva de los ataques DDoS y la necesidad de defensas robustas y especializadas.

AZ
2025

Los Malware:

.

Malware

- Software malicioso que daña o roba información.
- Tipos: virus, gusanos, troyanos, spyware, adware.
- Consecuencias: pérdida de información, espionaje, bajo rendimiento.

Software malicioso destinado a dañar o robar información.

AZ
2025

Los Malware:

- Antecedentes:
  El malware tiene una larga historia que se remonta a los años 70, cuando en 1971 Bob Thomas creó el programa Creeper, considerado el primer virus informático. Creeper era un experimento que se replicaba entre sistemas DEC PDP-10 a través de la red ARPANET y mostraba un mensaje divertido sin causar daño. Para contrarrestarlo, Ray Tomlinson creó Reaper, primer programa antivirus. En los 80 apareció Brain (1986), virus conocido de PC que se propagaba por disquetes, marcando la era inicial de virus informáticos dañinos. Con el crecimiento de Internet en los 90, el malware se sofisticó y proliferó, con virus masivos como ILOVEYOU en 1999, que provocó pérdidas millonarias a nivel global. Desde entonces, el malware ha evolucionado en formas y técnicas, transformándose en una amenaza constante para la seguridad informática.

AZ
2025

Los Malware:

- Concepto:
  Malware (software malicioso) es cualquier programa o código diseñado para infiltrarse, dañar o tomar control de sistemas informáticos sin consentimiento del usuario. Incluye virus, gusanos, troyanos, ransomware, spyware y adware. Puede robar información, dañar archivos, controlar dispositivos, cifrar datos para pedir rescate o espiar actividades. Es una de las principales herramientas del cibercrimen, destinada a causar perjuicios económicos, pérdida de información o daños a la privacidad.

AZ
2025

Los Malware:

- Casos relevantes:
- Virus ILOVEYOU (2000): Se propagó globalmente vía correo electrónico, cifrando archivos y provocando pérdidas multimillonarias.
- Gusano Morris (1988): Primer gran ataque de gusano que se propagó masivamente causando lentitud y caídas de redes.
- Ransomware WannaCry (2017): Afectó a más de 200,000 dispositivos en 150 países, con impacto en hospitales y empresas.
- Virus Mydoom (2004): Considerado uno de los más dañinos, causó daños por valor de miles de millones mediante ataques masivos a correos electrónicos.
- Ataques actuales: Sofisticados malwares dirigidos a infraestructura crítica, gobiernos y corporaciones, con técnicas avanzadas de evasión.

MODALIDADES DE DELITOS DIGITALES

1)

Acosadores Digitales:

Acosadores digitales:

1. **Acosadores digitales.-** Los acosadores digitales o ciberacosadores son individuos que utilizan medios y tecnologías digitales para hostigar, intimidar o acosar a otras personas. En el contexto peruano e internacional, están regulados por normativas que buscan proteger a las víctimas y sancionar estas conductas.

2. **Concepto y características de acosadores digitales.-** Los acosadores digitales actúan mediante medios electrónicos como redes sociales, correos electrónicos, chats, mensajes de texto y otras plataformas digitales para perseguir, vigilar o atacar psicológicamente a sus víctimas. Sus características comunes incluyen impulsividad, deseo de anonimato, manipulación, falta de empatía y obsesión por la víctima. Utilizan tecnología avanzada para obtener información personal, rastrear a la víctima y ejercer control o daño emocional.
3. **Instrumentos de acoso y tecnología digital.-**Los instrumentos usados para el acoso digital son variados: correos electrónicos, redes sociales, mensajes instantáneos, blogs, foros y sitios web maliciosos. Los acosadores pueden emplear técnicas como el rastreo de IP, virus informáticos, rootkits, registradores de teclas y perfiles falsos para recopilar y usar información privada o difamar a las víctimas.

AZ
2025

Acosadores digitales:

4. Normatividad nacional.-

Ley N° 30096 sobre delitos informáticos y modificaciones al Código Penal para castigar especialmente el acoso sexual a menores por medios digitales, estableciendo penas de hasta nueve años para acosadores que persigan fines sexuales contra menores de 14 años. También existe sanción para la difusión no autorizada de material audiovisual con contenido sexual, con penas de entre 2 a 15 años dependiendo del caso y edad de la víctima. Perú adhirió al Convenio de Budapest contra la ciberdelincuencia, reforzando la cooperación internacional para combatir estos delitos.

5. Normatividad internacional

El Convenio de Budapest sobre ciberdelincuencia es el principal tratado que combate el acoso en medios digitales, promoviendo la tipificación de delitos informáticos, mejora de técnicas investigativas y cooperación internacional. En la Unión Europea, directivas recientes amplían la protección contra el acoso digital y fortalecen los derechos de las víctimas, además de promover la seguridad y privacidad en el entorno digital.

Sanciones

Las sanciones para acosadores digitales en Perú varían según el delito y la víctima, incluyendo prisión desde dos hasta quince años en casos de acoso sexual, difusión de material sexual y acoso a menores. Internacionalmente, las penas pueden ser similares o complementarse con multas y medidas de restricción, con un enfoque en la protección de víctimas y prevención del delito mediante normas y directivas de cooperación entre países.

2)
APTs DIGITALES
Amenazas persistentes avanzadas

AZ
2025

2. APTs Digitales (Amenazas Persistentes Avanzadas).-

1. **APTs digitales (Amenazas Persistentes Avanzadas).-** Las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés) son ataques cibernéticos dirigidos, sofisticados y prolongados en el tiempo, diseñados para obtener acceso a sistemas informáticos con el fin de robar información confidencial, realizar ciberespionaje o sabotear infraestructuras críticas.
2. **Concepto y características de APT digitales.-**

Una APT se caracteriza por:

- Ser una amenaza avanzada que utiliza técnicas complejas como malware personalizado, exploits de día cero y métodos de infiltración sigilosos.
- Tener persistencia, es decir, los atacantes mantienen el acceso durante largos períodos — meses o años — para cumplir objetivos específicos.
- Operar de manera sigilosa para evitar detección y adaptarse a mecanismos defensivos.
- Buscar objetivos concretos, como estados, grandes empresas u organizaciones, para robar datos sensibles o sabotear operaciones.
- Utilizar múltiples vectores de ataque y procesos coordinados para lograr su objetivo.

Instrumentos y tecnología digital empleados.- Las APT emplean diversas herramientas tecnológicas:

- Malware avanzado y personalizado que puede incluir troyanos, rootkits y spyware.
- Exploits de vulnerabilidades, en especial de día cero.
- Técnicas de ingeniería social para penetrar en redes.
- Uso de vectores múltiples como correos electrónicos, redes, dispositivos físicos infectados
- exploits remotos para mantener el acceso

3)
Bot farms
(granjas de cuentas)

AZ
2025

3. Bot farms (granjas de cuentas)

Las bot farms o granjas de bots son redes de cuentas automatizadas controladas por una misma entidad para realizar actividades en línea a gran escala, muchas veces con fines de manipulación, fraude o acoso digital.

Concepto y características

Son conjuntos de bots, que son programas automatizados que realizan tareas repetitivas en internet.

Las granjas de bots manejan múltiples cuentas falsas para inflar seguidores en redes sociales, manipular tendencias, propagar noticias falsas o realizar ataques coordinados como DDoS.

Los bots en estas granjas pueden replicar patrones robotizados, publicar repetidamente, seguir cuentas específicas y generar interacción artificial.

Diferencian de trolls humanos, aunque pueden usarse conjuntamente para amplificar mensajes o desinformación.

Instrumentos y tecnología digital

Bots programados para publicar, dar "me gusta", compartir, seguir cuentas y enviar mensajes automáticos.

Software especializado para automatización masiva, manejo de cuentas falsas y ataques coordinados.

Pueden utilizar inteligencia artificial para simular comportamiento humano y evadir detección.

Incluyen herramientas para creación masiva de perfiles y gestión centralizada de bots.

AZ
2025

3. Bot farms (granjas de cuentas)

Normatividad peruana e internacional

En Perú, la Ley N° 31814 sobre inteligencia artificial regula el uso de tecnologías basadas en IA, estableciendo principios de ética, seguridad y responsabilidad.
La Ley N° 32314 sanciona el mal uso de IA para delitos incluyendo difamación y manipulación digital, que pueden aplicarse a acciones realizadas con bot farms.
No existe una tipificación específica para bot farms en la legislación peruana, pero se enmarcan en delitos informáticos y fraudes contemplados en la Ley de Delitos Informáticos y el Código Penal.

Internacionalmente, tratados y normas sobre delitos informáticos recomiendan regulación y sanción de estas prácticas en el marco de la lucha contra la desinformación y el abuso digital.

Sanciones

En Perú, las sanciones pueden incluir penas de prisión y multas para conductas fraudulentas o delictivas cometidas con bots, como manipulación de información o acoso.
Sanciones administrativas y civiles pueden aplicar a empresas y personas que utilicen bot farms para engañar usuarios o fraudar publicidad.
A nivel internacional, sanciones penales y económicas se aplican en la mayoría de países bajo leyes contra delitos informáticos y protección de datos.
En la práctica, muchas plataformas tecnológicas aplican bloqueos y restricción de cuentas automatizadas como medida de control.

4)
Botnets

AZ
2025

4. Botnets

Las botnets son redes de dispositivos informáticos infectados con malware que están controlados remotamente por un atacante para realizar actividades maliciosas coordinadas.

Concepto y características

Una botnet es un conjunto de computadoras o dispositivos comprometidos (bots o zombies) que un atacante controla de forma remota sin el consentimiento de los propietarios.
Se utilizan para realizar ataques distribuidos, como ataques de denegación de servicio (DDoS), envío masivo de spam, robo de información, distribución de malware y ciberespionaje.
Las botnets se caracterizan por su control remoto, capacidad de propagación, ocultamiento para evitar detección, robo de datos y actualización constante para mantenerse operativas.
Son difíciles de detectar y eliminar porque múltiples dispositivos controlados pueden continuar funcionando aunque algunos sean neutralizados.

Instrumentos y tecnología digital

Malware especializado infecta dispositivos para agregarlos a la botnet.
Herramientas para controlar múltiples bots simultáneamente, enviar comandos y ocultar la operación.
Técnicas que incluyen encriptación, uso de servidores de comando y control distribuidos, y actualizaciones continuas para evadir antivirus y detección.
Ataques comunes vía botnets incluyen DDoS, envío masivo de spam, phishing y minería ilícita de criptomonedas.

AZ
2025

4. Botnets

Normatividad peruana e internacional

En Perú, las botnets están reguladas dentro del marco de delitos informáticos previsto por la Ley N° 30096 y el Código Penal, que sancionan accesos indebidos, sabotaje informático y delitos relacionados.

No existe una tipificación específica para botnets, pero sus actividades ilícitas están contempladas como ciberdelitos y fraudes digitales.

Perú cuenta con normativas complementarias en ciberseguridad y participa en tratados internacionales como el Convenio de Budapest, que establecen cooperación para combatir estos delitos.

A nivel internacional, leyes y tratados multilaterales regulan la persecución de delitos cometidos con botnets, estableciendo sanciones penales, civiles y administrativas.

Sanciones

Las sanciones en Perú pueden incluir prisión y multas para quienes operen o utilicen botnets con fines ilícitos, como ataques, robo de información o sabotaje.

Pueden aplicarse también sanciones administrativas a personas jurídicas y responsables de seguridad informática.

Internacionalmente, se imponen penas similares, con énfasis en la cooperación transfronteriza para detener operadores de botnets y mitigar sus impactos.

Las plataformas tecnológicas y proveedores de servicios suelen adoptar medidas técnicas para detectar y bloquear botnets.

5.
Botseadores digitales

AZ
2025

5. Bots eadores digitales

Los bots digitales son programas automatizados diseñados para realizar tareas repetitivas y específicas en internet, con aplicaciones tanto legítimas como maliciosas en el ecosistema digital.

Concepto y características de bots digitales

Son software automatizado que ejecutan acciones como buscar, recopilar información, interactuar en redes sociales o procesar datos.

Presentan diversidad: desde bots de búsqueda para indexar sitios web (rastreadores), scrapers que extraen datos específicos, hasta chatbots que mantienen conversaciones simulando humanos.

Algunos bots utilizan inteligencia artificial para adaptarse y simular comportamientos humanos complejos.

Operan a gran velocidad y escala, conectándose con diferentes plataformas y sistemas mediante APIs y protocolos estandarizados.

Pueden ser herramientas útiles para empresas, periodistas y usuarios, pero también pueden usarse para acoso, manipulación, spam y fraudes en línea.

Instrumentos de acoso y tecnología digital

Bots maliciosos pueden crear perfiles falsos en redes sociales, enviar mensajes no deseados, reproducir contenido repetitivo o manipular tendencias online.

La tecnología tras estos bots incluye programación avanzada, algoritmos de inteligencia artificial, redes de comunicación y técnicas para evadir detección.

Se usa desde simples scripts hasta sistemas complejos integrados con machine learning para

AZ
2025

5. Bots eadores digitales

Normatividad peruana e internacional

En Perú, la legislación comienza a abordar el uso de bots en su normativa sobre inteligencia artificial (Ley N° 31814) que establece principios para un uso ético y controlado de tecnologías automatizadas.

No existen leyes específicas que regulen bots en general, pero su uso malicioso puede ser sancionado en el marco de la Ley de Delitos Informáticos (Ley N° 30096) y Código Penal, donde se tipifican conductas como el acoso, fraude informático, usurpación de identidad o manipulación digital.

Internacionalmente, tratados como el Convenio de Budapest establecen directrices para combatir delitos tecnológicos, incluyendo el uso abusivo de bots para actividades ilícitas.

La normatividad enfatiza la necesidad de transparencia, responsabilidad y protección a la privacidad y derechos digitales.

Sanciones

En Perú, las sanciones pueden incluir penas privativas de libertad y multas para quienes usen bots para cometer delitos informáticos, acoso, difamación o manipulación fraudulenta.

Se consideran tanto sanciones penales como administrativas dependiendo del caso y la gravedad.

A nivel internacional, las sanciones se complementan con bloqueo de cuentas, medidas contra fraudes y cooperación para persecución transnacional.

Plataformas digitales aplican medidas técnicas para detección, bloqueo y mitigación del uso malicioso de bots.

6.

Ciberdelincuentes organizados

AZ
2025

6. Ciberdelincuentes organizados

Los ciberdelincuentes organizados son grupos estructurados que ejecutan actividades delictivas en el entorno digital de manera coordinada y con objetivos específicos, utilizando tecnologías avanzadas para cometer delitos informáticos.

Concepto y características

Se componen de varios miembros con roles definidos, como hackers, expertos en sistemas, operadores financieros y especialistas en ocultamiento digital.
Sus actividades incluyen el robo de datos personales y financieros, ransomware, fraude en línea, ciberextorsión, venta ilegal de bienes digitales y piratería informática.
Actúan con sofisticación, planeación y persistencia, utilizando técnicas como phishing, malware avanzado y ataques DDoS.
Estos grupos operan a nivel transnacional, aprovechando el anonimato relativo de internet para dificultar su rastreo.
Pueden estar vinculados con organizaciones criminales tradicionales o ser autónomos con fines económicos o políticos.

Instrumentos de acoso y tecnología digital

Usan herramientas digitales como malware, ransomware, troyanos, botnets, phishing y exploit kits para atacar objetivos.
Emplean redes ocultas (darknet), plataformas de comunicación segura, criptomonedas para lavados financieros, y técnicas de anonimato como VPNs y servicios TOR.
Su arsenal tecnológico incluye tecnologías de cifrado, automatización de ataques y evasión de controles.

AZ
2025

6. Ciberdelincuentes organizados

Normatividad peruana e internacional

Perú tipifica y sanciona los delitos de ciberdelincuencia a través de la Ley N° 30096 y sus modificaciones, que incluyen delitos de acceso ilícito, daño informático, fraude electrónico y lavado de activos vinculados a la tecnología.

Participa en convenios internacionales como el Convenio de Budapest para fortalecer la cooperación en la persecución de delitos cibernéticos.

La legislación peruana se complementa con regulaciones sobre protección de datos, uso de inteligencia artificial, y medidas administrativas para proteger infraestructuras críticas.

A nivel global, los marcos normativos incluyen tratados multilaterales que buscan armonizar la persecución y sanción de ciberdelitos organizados, incluyendo aspectos de colaboración judicial y policial.

Sanciones

Las sanciones en Perú para ciberdelincuentes organizados pueden incluir prisión efectiva, multas significativas y confiscación de bienes, con agravantes cuando afecten a menores, el Estado o sectores estratégicos.

Existen sanciones administrativas y procesos civiles complementarios para la reparación del daño.

A nivel internacional, se aplican sanciones similares con énfasis en combatir el lavado de dinero digital y fortalecer colaboraciones judiciales.

Las sanciones buscan no sólo castigar, sino desarticular las redes criminales y prevenir futuros ataques.

7. Ciberterrorista

AZ
2025

7. Ciberterrorista

El ciberterrorismo es una modalidad de criminalidad que utiliza tecnologías de la información y comunicación (TIC) para cometer actos terroristas con el fin de infundir miedo, causar daños graves o desestabilizar sistemas críticos, tanto de infraestructura pública como privada.

Concepto y características

El ciberterrorismo implica el uso malicioso de herramientas digitales para ataques que afectan la seguridad nacional, infraestructuras críticas o bienes y servicios esenciales.
Se caracteriza por realizar ataques informáticos destructivos, como sabotajes a sistemas de energía, agua, telecomunicaciones o sistemas financieros.
Incluye también la propagación de propaganda terrorista, reclutamiento, espionaje digital y ataques de denegación de servicio (DDoS).
Su objetivo es causar miedo, daño económico, social o político, y desestabilizar gobiernos o sociedades.
Se ejecuta mediante técnicas como malware avanzado, troyanos, virus, phishing, y ataques coordinados en redes.

Instrumentos de acoso y tecnología digital

Se emplean programas maliciosos, virus, ransomware, troyanos, herramientas de control remoto y bots para infiltrarse en sistemas.
Uso de redes ocultas (dark web) para coordinar ataques y financiarse mediante criptomonedas.
Tecnologías de cifrado, anonimato (VPN, Tor) y comunicaciones seguras para ocultar identidad y operación.
Se utilizan también tecnologías de ingeniería social para reclutar y difundir mensajes.

AZ
2025

7. Ciberterrorista

Normatividad peruana e internacional

En Perú, el ciberterrorismo está incluido en la Ley N° 30096 y el Código Penal bajo disposiciones relativas a delitos informáticos, terrorismo y sabotaje a infraestructuras críticas.

A nivel internacional, la normatividad para enfrentar el ciberterrorismo está contenida en tratados multilaterales como el Convenio de Budapest y regulaciones específicas de ciberseguridad y lucha contra el terrorismo.

Las leyes nacionales se complementan con protocolos y acuerdos para la cooperación internacional en la prevención, investigación y sanción del ciberterrorismo.

Perú ha sido cauteloso en la implementación de un marco legal específico para el ciberterrorismo, pero ha avanzado en políticas de ciberseguridad y defensa digital.

Sanciones

Las sanciones para actos de ciberterrorismo en Perú incluyen penas de prisión severas, multas y confiscación de bienes relacionados con la actividad criminal.

Se consideran agravantes el daño a menores, a infraestructuras críticas y la vinculación con organizaciones terroristas.

A nivel internacional, las sanciones incluyen además medidas de bloqueo económico y ciberdefensa coordinada.

Los sistemas judiciales buscan la prevención y desarticulación de redes terroristas digitales junto con protección a la población y a los sistemas nacionales.

8. Crackers

AZ
2025

8. Crackers

Los crackers son personas con conocimientos avanzados en informática que acceden a sistemas sin autorización con fines maliciosos, buscando causar daño, robar información o beneficios económicos ilícitos.

Concepto y características

El cracker es distinto del hacker ético; mientras el hacker busca mejorar la seguridad, el cracker se enfoca en vulnerar sistemas para actividades ilegales.
Utilizan programas para detectar y explotar vulnerabilidades, diseñan herramientas intrusivas y pueden destruir o robar información.
Son motivados por fines económicos, reconocimiento en comunidades ilícitas o simplemente causar daño.
Operan sin ética, violan la privacidad y pueden compartir o vender la información robada.
Su modus operandi incluye hackeo, introducción de malware, ransomware, y acceso no autorizado, con un perfil delictivo común en la ciberdelincuencia.

Instrumentos y tecnología digital

Utilizan software para análisis de vulnerabilidades, exploits, rootkits, keyloggers, troyanos y malware personalizado.
La tecnología abarca desde scripts básicos hasta avanzados kits de explotación y herramientas de sigilo para evadir detección.
Sus acciones pueden incluir también phishing, ataques DDoS y difusión de información robada en la deep web.
Pueden emplear redes de bots o botnets para ampliar el alcance y efectividad de sus ataques

AZ
2025

8. Crackers

Normatividad peruana e internacional

En Perú, los crackers son sancionados bajo leyes de delitos informáticos, como la Ley N° 30096 y disposiciones del Código Penal que tipifican el acceso ilícito, daño informático y fraudes relacionados.

Internacionalmente, el Convenio de Budapest y otros tratados regulan y promueven la cooperación para combatir a estos ciberdelincuentes.

Las normativas incluyen responsabilidad penal, protección de datos y medidas para prevenir la ciberdelincuencia.

No existen normas específicas solo para crackers, pero se aplica la legislación general contra delitos informáticos y fraudes tecnológicos.

Sanciones

Las sanciones penales para crackers en Perú incluyen prisión efectiva para quienes vulneren sistemas y cometan delitos cibernéticos con fines ilícitos.

Se contemplan multas, confiscación de bienes y procesos civiles para reparación de daños.

A nivel internacional, sanciones complementarias involucran acuerdos para extradición, bloqueo financiero y cooperación en investigaciones.

Se acompañan con medidas técnicas preventivas y de detección para mitigar sus ataques y proteger a las víctimas.

En conclusión, los crackers son ciberdelincuentes que usan técnicas de intrusión informática con fines maliciosos, regulados en Perú y a nivel internacional bajo leyes de delitos informáticos, con sanciones penales y administrativas para combatir su impacto ilegal.

9. Cyborg delincuentes

AZ
2025

9. Cyborg delincuentes

Los ciberdelincuentes cyborg son individuos o entidades que combinan capacidades humanas con tecnologías digitales avanzadas para ejecutar actos ilícitos en el ciberespacio, configurando un híbrido entre humano y máquina en la comisión delictiva.

Concepto y características

El término "cyborg delincuente" refiere a la fusión hombre-máquina donde el sujeto utiliza interfaces digitales para realizar delitos, aumentando sus capacidades mediante tecnología.
Se consideran actores que operan en el ciberespacio con un fuerte componente tecnológico, usando automatización e inteligencia artificial junto con habilidades humanas.
Presentan comportamientos complejos, incluyendo la utilización de algoritmos autónomos o semiautónomos que pueden operar con limitada intervención humana.
Incluyen conductas desviadas propias del entorno digital como adicción, obsesiones, y manipulación tecnológica para cometer cibercrímenes.
Este perfil va más allá de la simple cibercriminalidad, implicando aspectos filosóficos y sociales sobre la interacción humano-tecnología en el delito.

Instrumentos y tecnología digital

Uso de interfaces humano-máquina, software autónomo y algoritmos de decisión automatizada para ataques y fraudes.
Robots digitales, bots avanzados, redes distribuidas y sistemas basados en IA para infiltración, evasión y manipulación.
Tecnología empleada para crear automatismos en la ejecución de delitos, incluso con cierto grado de autogestión o "decisión" propia.

AZ
2025

9. Cyborg delincuentes

Normatividad peruana e internacional

No existe en Perú una legislación específica que regule la figura del delincuente cyborg, pero sus actos se encuadran dentro del marco general de delitos informáticos contemplados en la Ley N° 30096 y Código Penal.

La normatividad internacional, a través del Convenio de Budapest y otras iniciativas, abarca la persecución de cibercrímenes cometidos con asistencia tecnológica avanzada.

La complejidad de atribución de responsabilidad en delitos realizados con automatismos genera desafíos legales, especialmente cuando los actos delictivos se ejecutan parcialmente por sistemas autónomos.

Existe un debate jurídico y filosófico sobre la imputabilidad penal de actos realizados con la intervención parcial o total de sistemas automáticos o IA.

Sanciones

En Perú, las sanciones aplican conforme a la legislación cibernética para delitos cometidos con apoyo tecnológico, incluyendo prisión y multas, aunque sin regulación específica para ciberdelincuentes cyborg.

A nivel internacional, se buscan mecanismos para actualizar marcos legales que contemplen la responsabilidad en delitos con componentes de automatización y IA.

Las sanciones buscan tanto castigar como prevenir este tipo complejo de ciberdelincuencia, fomentando cooperación internacional y desarrollo tecnológico defensivo.

En síntesis, los ciberdelincuentes cyborg representan un perfil híbrido de delincuencia donde la tecnología extendida potencia la capacidad criminal, con un marco normativo peruano e internacional que adapta leyes tradicionales a estos nuevos escenarios, aunque con retos legales sobre imputabilidad y regulación específica.

10. Delicuentes ciberneticos de cuello blanco

AZ
2025

10. Delicuentes ciberneticos de cuello blanco

Los delincuentes cibernéticos de cuello blanco son individuos que, generalmente con alto estatus social y profesional, cometen delitos informáticos aprovechando su posición y conocimientos para obtener beneficios ilícitos mediante fraudes, corrupción o abuso de confianza en el ámbito digital.

Concepto y características

Provienen de sectores profesionales o empresariales y cometen delitos en el ejercicio de sus funciones o actividades económicas.
Son respetados socialmente, con educación formal y estatus económico elevado.
Sus delitos no suelen implicar violencia física pero causan daños económicos significativos y violan la confianza pública o privada.
Utilizan su conocimiento técnico y posición para perpetrar fraudes, lavado de dinero, corrupción, malversación y delitos informáticos sofisticados.
Se caracterizan por planear y ejecutar conductas ilícitas en entornos digitales de forma oculta y organizada.

Instrumentos y tecnología digital

Emplean sistemas informáticos para manipular registros contables, ocultar transacciones ilícitas, crear sociedades fantasmas o manipular información financiera.
Usan software especializado para acceso y control de sistemas, phishing, ingeniería social, malware para filtración de datos y encubrimiento digital.
Utilizan plataformas digitales para lavado de activos, transferencia electrónica y ocultamiento de actividades

AZ
2025

10. Delicuentes ciberneticos de cuello blanco

Normatividad peruana e internacional

Perú sanciona estos delitos dentro del marco de la Ley N° 30096 y el Código Penal, que tipifican delitos como fraude informático, lavado de activos, corrupción y abuso de confianza. También hay regulaciones específicas para la prevención de lavado de activos con apoyo de tecnología financiera.

A nivel internacional, se aplican convenios multilaterales para combatir la delincuencia de cuello blanco digital, como la Convención de las Naciones Unidas contra la Corrupción y el Convenio de Budapest.

Estos marcos buscan cooperación internacional para la investigación, persecución y sanción de estos delitos que trascienden fronteras.

Sanciones

Las sanciones en Perú incluyen penas privativas de libertad, multas importantes, decomiso de bienes y medidas administrativas en contra de responsables.

Se contempla agravantes según el nivel de daño económico, jerarquía del delincuente y si afectan al sector público o privado con consecuencias sociales graves.

A nivel internacional, se aplican penas similares y mecanismos de cooperación jurídica para judicializar casos transnacionales.

Las sanciones buscan desalentar la comisión de delitos económicos y proteger la integridad del sistema financiero y social.

En resumen, los delincuentes cibernéticos de cuello blanco son actores de alto perfil social que cometen delitos informáticos con sofisticación, regulados en Perú y en ámbitos internacionales dentro del marco de delitos económicos y cibernéticos, con sanciones penales y administrativas que buscan la reparación del daño y la prevención.

11. Delincuentes oportunistas

AZ
2025

11. Delincuentes oportunistas

Los delincuentes cibernéticos oportunistas son aquellos que aprovechan vulnerabilidades o situaciones momentáneas para cometer delitos informáticos sin planificación previa ni objetivos específicos a largo plazo. Actúan aprovechando oportunidades que se presentan sin un conocimiento profundo o preparación técnica avanzada, buscando beneficios rápidos.

Concepto y características

Definidos por su conducta reactiva y circunstancial, atacan sistemas o víctimas sin un plan estructurado.

Su acción es muchas veces impulsiva, respondiendo a brechas de seguridad momentáneas o accesos fáciles.

Pueden ser individuos con conocimientos básicos o hackers menos especializados que explotan vulnerabilidades simples.

Sus ataques son generalmente indiscriminados y poco sofisticados, pero pueden causar daño significativo a víctimas desprevenidas.

Usan técnicas comunes de ciberdelincuencia como phishing, malware básico, ransomware oportunista y esquemas de fraude digital.

Instrumentos y tecnología digital

Herramientas accesibles públicamente y software malicioso común, kits de explotación conocidos y mensajes fraudulentos automatizados.

Emplean técnicas de ingeniería social, mensajes de phishing, smishing, y malware de propagación fácil.

Suelen valerse de redes Wi-Fi abiertas, credenciales débiles y vulnerabilidades no parcheadas

AZ
2025

11. Delincuentes oportunistas

Normatividad peruana e internacional

En Perú, estos actos se regulan bajo las leyes de delitos informáticos, principalmente la Ley N° 30096 y el Código Penal, que contemplan ataques tanto sofisticados como básicos.

La normatividad internacional en materia de cibercrimen también incluye medidas para sancionar todo tipo de delitos, sin importar su grado de planificación.

Se promueven políticas de ciberseguridad para fortalecer la prevención y detección, poniendo énfasis en la educación digital y fortalecimiento institucional.

La cooperación internacional busca combatir la variedad de ciberataques, incluidos los oportunistas que pueden actuar en cualquier momento y lugar.

Sanciones

Las sanciones aplican de forma general para todos los delitos informáticos, con penas de prisión, multas y medidas de reparación.

Aunque los delitos de oportunistas pueden ser considerados menos graves, el daño causado a víctimas puede justificar sanciones proporcionales.

Se busca disuadir cualquier tipo de ataque, promoviendo el fortalecimiento de controles junto con sanciones ejemplares.

Las plataformas digitales y organismos reguladores aplican bloqueos, denuncias y otras respuestas técnicas para mitigar impactos.

En resumen, los delincuentes cibernéticos oportunistas actúan aprovechando cualquier oportunidad para cometer delitos básicos en el entorno digital, regulados en Perú y globalmente con sanciones que cubren toda la gama de cibercrímenes, con un enfoque preventivo y punitivo acorde a los daños causados.

12. Gusanistas

AZ
2025

12. Gusanistas

Los "gusanistas" no son propiamente delincuentes, sino que el término está relacionado con los gusanos informáticos, que son programas maliciosos que se replican a sí mismos y se propagan a través de redes para infectar múltiples sistemas.

Concepto y características

Un gusano informático es un malware autónomo que se replica y propaga automáticamente por redes, a diferencia del virus que requiere activación en un equipo host.
Utiliza vulnerabilidades de sistemas operativos o redes para propagarse sin el conocimiento del usuario.
Puede transportar cargas útiles maliciosas como ransomware, virus o puertas traseras para tomar control de sistemas infectados.
Consume recursos de red y hardware, afectando el rendimiento y disponibilidad de sistemas.
Se propaga normalmente a través de correos electrónicos con archivos adjuntos maliciosos, mensajes instantáneos u otros medios digitales de comunicación para llegar a nuevas víctimas.

Instrumentos y tecnología digital

Explota vulnerabilidades del sistema operativo o software instalado.
Se camufla en archivos aparentemente inocuos o urgentes para engañar al usuario (ingeniería social).
Puede incluir técnicas para evadir antivirus y sistemas de detección.
Participa en ataques coordinados como DDoS al utilizar sistemas infectados para inundar redes o servicios.
Algunos gusanos se integran en redes de bots para amplificar su alcance y daño.

AZ
2025

12. Gusanistas

Normatividad peruana e internacional

La propagación de gusanos informáticos se encuadra en delitos informáticos según la Ley N° 30096 y el Código Penal peruano, que prohíben la creación, distribución y uso de malware.

A nivel internacional, convenios como el Convenio de Budapest regulan la sanción de la creación y difusión de estos programas maliciosos.

La legislación busca proteger la integridad y disponibilidad de sistemas de información frente a malware autorreplicante.

Se promueve la cooperación internacional para la investigación, prevención y persecución de estos delitos.

Sanciones

En Perú, las sanciones incluyen prisión y multas para quienes desarrollen, distribuyan o usen gusanos informáticos con fines ilícitos.

Se aplican medidas de prevención y control para evitar la propagación y mitigar daños.

A nivel global, sanciones penales y administrativas buscan la disuasión y protección de infraestructuras críticas y usuarios.

Las sanciones también abarcan la reparación del daño, confiscación de equipos y restricciones de actividades tecnológicas.

En resumen, los gusanistas se relacionan con la propagación de gusanos informáticos, malware capaz de replicarse y causar daños en redes y sistemas. Este fenómeno está regulado en Perú y a nivel internacional dentro de las leyes contra delitos informáticos, con sanciones penales y administrativas para quien los utilice maliciosamente.

13. Hacker

AZ
2025

13. Hacker

Un hacker es una persona con profundo conocimiento técnico en informática que utiliza sus habilidades para explorar, analizar y modificar sistemas informáticos. La definición no implica necesariamente intenciones ilícitas; existen hackers éticos que fortalecen la seguridad y hackers maliciosos que explotan vulnerabilidades para realizar ataques.

Concepto y características

Un hacker posee habilidades avanzadas en programación, redes y sistemas, enfocándose en detectar vulnerabilidades y mejorar o vulnerar la seguridad.
Sus actividades pueden ir desde innovar en tecnologías, mejorar sistemas de protección, hasta realizar intrusiones con fines ilegítimos.
Se diferencian tipos de hackers: de sombrero blanco (éticos), sombrero negro (maliciosos), y sombrero gris (intermedios).
Los hackers exploran los límites tecnológicos para crear soluciones o, en casos negativos, para causar daños, robo de información o sabotaje.

Instrumentos y tecnología digital

Utilizan herramientas como software para pruebas de penetración, análisis de vulnerabilidades, exploits, troyanos y malware.
Pueden realizar ataques de denegación de servicio (DDoS), phishing, ingeniería social y accesos remotos no autorizados.
Emplean técnicas sofisticadas para evadir detección y preservar anonimato.

AZ
2025

13. Hacker

Normatividad peruana e internacional

En Perú, no existe una definición legal única para hackers, pero sus actos pueden estar tipificados como delitos informáticos bajo la Ley N° 30096 y disposiciones del Código Penal.

Normativas internacionales como el Convenio de Budapest promueven la cooperación en la persecución de cibercrímenes, incluyendo ataques realizados por hackers con intenciones maliciosas.

La legislación peruana establece que el uso ilícito de estas habilidades puede ser sancionado, mientras que el hacking ético es promovido para fortalecer la ciberseguridad.

Sanciones

Las sanciones penales en Perú incluyen prisión y multas para quienes realicen accesos no autorizados, daño informático, fraude y otros ciberdelitos.

A nivel internacional se aplica una gama similar de sanciones y se promueven acuerdos para la colaboración en la represión y prevención de delitos informáticos.

También existen sanciones administrativas y medidas técnicas para proteger los sistemas y usuarios.

En conclusión, un hacker es un experto en tecnología que puede ser tanto un defensor de la seguridad como un atacante. Perú y la normativa internacional regulan sus actividades para castigar los actos ilícitos y fomentar los usos éticos de sus habilidades.

14. Hackers Black Hat (Sombrero Negro)

AZ
2025

14. Hackers Black Hat (Sombrero Negro)

Los hackers de sombrero negro (black hat hackers) son individuos que utilizan sus habilidades técnicas para vulnerar sistemas informáticos sin autorización, con el fin de obtener beneficios ilícitos, causar daño o sabotear redes.

Concepto y características

Actúan de manera ilegal, sin consentimiento, para acceder, manipular o destruir información.
Buscan principalmente lucro económico, espionaje, sabotaje o difusión de malware.
Operan en la clandestinidad, utilizando técnicas avanzadas para evadir detección y anonimato.
Son expertos en explotar vulnerabilidades no parchadas en software y sistemas.
Se caracterizan por utilizar métodos de ingeniería social, phishing, malware, ransomware y ataques DDoS.

Instrumentos y tecnología digital

Malware (virus, troyanos, ransomware, keyloggers).
Exploits para infiltrarse en sistemas vulnerables.
Ingeniería social y phishing para obtener credenciales.
Redes IoT comprometidas y botnets para ataques masivos.
Herramientas para ocultar su identidad, como VPNs y la dark web.

15. Hackers Blue Hat (sombrero azul)

AZ
2025

15. Hackers Blue Hat (sombrero azul)

Los hackers de sombrero azul (Blue Hat) son especialistas que realizan pruebas de seguridad, generalmente contratados externamente por organizaciones para detectar vulnerabilidades en sistemas informáticos antes de que sean lanzados o expuestos públicamente.

Concepto y características

No forman parte del equipo interno de la organización, sino que actúan como evaluadores externos.

Su objetivo es identificar fallas de seguridad para que sean corregidas, permitiendo fortalecer la protección del sistema.

A diferencia de los hackers de sombrero blanco (White Hat), cuya función es continua dentro de la organización, los Blue Hat suelen participar en auditorías o pruebas específicas.

En otro contexto, el término también se usa para referirse a hackers con intención vengativa, que atacan sin buscar lucro económico, afectando la confianza o continuidad de negocios o personas.

Los Blue Hat éticos trabajan con autorización y buscan evitar daños mediante la detección temprana de vulnerabilidades.

Instrumentos y tecnología digital

Herramientas de análisis y pruebas de penetración (pentesting).

Software para escaneo de puertos, análisis de vulnerabilidades, simulación de ataques.

Técnicas de ingeniería social para evaluar la seguridad humana.

Plataformas de prueba y ambientes controlados para testear defensas sin comprometer la información sensible.

AZ
2025

15. Hackers Blue Hat (sombrero azul)

Normatividad peruana e internacional

En Perú, las actividades de pruebas y auditoría de seguridad son legales cuando se realizan con autorización, reguladas por la Ley N° 30096 y el Código Penal en aspectos de autorización y consentimiento.

La normatividad internacional también contempla la existencia de pruebas de pentesting y auditorías como parte de buenas prácticas en ciberseguridad.

El marco legal destaca la importancia del consentimiento y la legalidad para distinguir estas prácticas de ataques ilegales.

Perú y tratados internacionales promueven este tipo de actividades para fortalecer la protección a infraestructuras críticas.

Sanciones

Para hackers Blue Hat éticos no hay sanciones, ya que su actividad se realiza con consentimiento y tiene fines legítimos.

La falta de autorización o cualquier acción no consentida que cause daño sí es sancionada penalmente.

Las sanciones para actividades no autorizadas se aplican conforme a leyes de delitos informáticos en Perú y otros países.

Se promueven políticas y certificaciones para formar y regular la actuación de estos especialistas.

En resumen, los hackers Blue Hat son profesionales que realizan pruebas externas de seguridad con autorización para mejorar sistemas, regulados en Perú e internacionalmente bajo leyes que los distinguen de actos ilícitos, sin sanciones cuando actúan legalmente.

16. Hackers éticos (White Hat)

AZ
2025

16. Hackers éticos (White Hat)

Los hackers éticos, también conocidos como hackers de sombrero blanco (White Hat), son profesionales de la ciberseguridad que utilizan sus habilidades para identificar y corregir vulnerabilidades en sistemas informáticos con el consentimiento legal de los propietarios, con el objetivo de proteger las redes, datos y sistemas contra ataques maliciosos.

Concepto y características

Los hackers éticos tienen conocimientos técnicos profundos similares a los hackers maliciosos, pero su intención es proteger y no dañar.
Realizan pruebas de penetración para detectar fallas en la seguridad y ayudan a implementar las medidas necesarias para corregirlas.
Trabajan con autorización expresa y dentro de un marco ético y legal.
Su función es preventiva y colaborativa, apoyando a organizaciones públicas y privadas para fortalecer sus defensas.
Se diferencian claramente de los hackers de sombrero negro (Black Hat), quienes hacen intrusiones maliciosas sin consentimiento.

Instrumentos y tecnología digital

Usan herramientas legítimas de análisis de vulnerabilidades, escáneres de seguridad, simuladores de ataques y software especializado para pruebas de penetración.
Emplean técnicas avanzadas de hacking ético, como ingeniería social controlada, evaluación de políticas de seguridad y análisis forense.
Trabajan en ambientes controlados y con permisos para evitar daños colaterales.
Ayudan también en la capacitación y desarrollo de protocolos de seguridad efectivos basados

AZ
2025

16. Hackers éticos (White Hat)

Normatividad peruana e internacional

En Perú, estas actividades están reguladas bajo la Ley N° 30096 y el Código Penal, que permiten la realización de pruebas de seguridad informática con consentimiento.

La legislación peruana promociona el hacking ético para mejorar la ciberseguridad nacional y proteger infraestructuras críticas.

A nivel internacional, tratados como el Convenio de Budapest reconocen y fomentan la cooperación y el uso ético de estas prácticas para la prevención del cibercrimen.

La regulación distingue claramente entre actividades autorizadas y aquellas sin consentimiento, que sí son sancionables.

Sanciones

Los hackers éticos que actúan con consentimiento y dentro del marco legal no enfrentan sanciones.

Las actividades similares realizadas sin autorización constituyen delitos informáticos con sanciones penales.

Las leyes buscan promover el desarrollo profesional de hackers éticos mediante certificaciones y formación.

La cooperación internacional también impulsa normativas y estándares para el hacking ético.

En resumen, los hackers éticos (white hat) son profesionales que usan sus competencias con fines legítimos para fortalecer la seguridad informática, regulados en Perú e internacionalmente bajo normativas que promueven su trabajo y sancionan el hacking malicioso.

17. Hackers Green Hat (sombrero verde)

AZ
2025

17. Hackers Green Hat (sombrero verde)

Los hackers de sombrero verde (Green Hat) son aficionados o principiantes en el mundo del hacking, quienes están en proceso de aprendizaje y desarrollo para llegar a ser hackers más avanzados, ya sea éticos (White Hat) o maliciosos (Black Hat).

Concepto y características

Son inexpertos, todavía aprendiendo técnicas de hacking y seguridad informática.
Su objetivo principal es adquirir habilidades, conocimientos y experiencia en hacking.
Pueden aspirar a convertirse en hackers éticos (de sombrero blanco) o maliciosos (de sombrero negro) según su ética y decisiones futuras.
No tienen un enfoque claro ni consolidado en actuar ni para proteger ni para atacar.
A menudo utilizan herramientas y scripts ya desarrollados por otros, por lo que se les conoce también como "script kiddies".

Instrumentos y tecnología digital

Utilizan herramientas automatizadas y disponibles públicamente para explorar sistemas y redes.
No suelen desarrollar sus propios exploits o software, sino que replican métodos ya existentes.
Suelen usar programas de escaneo, ataques básicos de fuerza bruta, y técnicas sencillas de phishing.
Están en etapas tempranas de su aprendizaje tecnológico, por lo que su impacto puede ser limitado aunque no despreciable.

AZ
2025

17. Hackers Green Hat (sombrero verde)

Normatividad peruana e internacional

En Perú, los actos de hacking sin autorización son sancionados conforme a la Ley N° 30096 y el Código Penal, por lo que acciones realizadas por green hats si son ilícitas pueden generar responsabilidad penal.

La legislación no distingue específicamente a hackers de sombrero verde, pero los regula en el marco general de delitos informáticos.

A nivel internacional, las normativas abordan el uso no autorizado de sistemas y la comisión de delitos cibernéticos sin importar el nivel técnico del infractor.

Se promueve la formación y orientación ética para que estos aprendices evolucionen hacia prácticas legales y legítimas.

Sanciones

Las sanciones para infracciones cometidas por hackers green hat incluyen penas de prisión, multas y medidas legales según la gravedad y consecuencias de sus actos.

La legislación procura disuadir conductas ilegales incluso de aprendices o menores de edad, con sanciones proporcionales.

Se fomentan programas educativos para darles alternativas legales y aprovechar su interés por la tecnología.

En resumen, los hackers de sombrero verde son aprendices en hacking con potencial para desarrollarse en el campo, regulados legalmente en Perú e internacionalmente como sujetos de delitos informáticos cuando cometen actos ilícitos, con sanciones aplicables según la legislación vigente.

18. Hackers Grey Hat (Sombrero Gris)

AZ
2025

18. Hackers Grey Hat (Sombrero Gris)

Los hackers de sombrero gris (Grey Hat) son una categoría intermedia entre los hackers éticos (White Hat) y los hackers maliciosos (Black Hat). Actúan a menudo sin autorización, pero sin intenciones maliciosas claras, buscando descubrir vulnerabilidades y a veces notificarlas, aunque de forma no siempre ética o legal.

Concepto y características

Son hackers talentosos que acceden a sistemas sin permiso legal, pero sin intención de causar daño o lucro ilícito.
Suelen descubrir vulnerabilidades para evidenciar fallas de seguridad y presionar a las organizaciones a corregirlas.
A veces hacen públicas las vulnerabilidades sin autorización, lo que genera controversia ética y legal.
Actúan en una zona gris entre el bien y el mal, con métodos cuestionables pero motivaciones que pueden ser consideradas como de "bien común".
Suelen ser vistos con recelo tanto por hackers éticos, que desaprueban la ilegalidad, como por hackers maliciosos, por la falta de beneficio personal directo.

Instrumentos y tecnología digital

Usan técnicas avanzadas para penetrar redes y sistemas, igual que hackers black hat, como ingeniería social, exploits, malware y análisis de vulnerabilidades.
Emplean herramientas para escanear sistemas, identificar puntos débiles, y a veces software automatizado para difundir vulnerabilidades.
Su actividad incluye a menudo pruebas de intrusión no autorizadas para descubrir fallos de

AZ
2025

18. Hackers Grey Hat (Sombrero Gris)

Normatividad peruana e internacional

En Perú, aunque los actos de hackers de sombrero gris son ilegales por realizarlos sin autorización, no hay una regulación específica para ellos.

Están tipificados dentro de los delitos informáticos regulados por la Ley N° 30096 y el Código Penal respecto a acceso no autorizado y daño informático.

Internacionalmente, el Convenio de Budapest abarca delitos de acceso indebido, pero también promueve la colaboración para fortalecer sistemas contra estos ataques.

El debate legal se centra en la responsabilidad penal frente a las motivaciones y consecuencias de sus actos.

Sanciones

Se pueden imponer penas de prisión y multas por acceso indebido, incluso si no hubo daño directo o lucro.

No siempre se aplican sanciones cuando se evidencia buena fe, pero eso depende de las autoridades y contextos específicos.

Las sanciones buscan proteger la seguridad, privacidad y estabilidad de sistemas frente a intervenciones no autorizadas.

La cooperación internacional busca equilibrar la prevención de daños y la promoción de prácticas responsables.

En conclusión, los hackers de sombrero gris son actores legales ambiguos que exploran sistemas sin autorización, motivados por la mejora de la seguridad pero con métodos irregulares. Están regulados bajo leyes de delitos informáticos en Perú e internacionalmente, con sanciones aplicables según los efectos y contextos de sus acciones.

19. Hackers Red Hat (sombrero rojo)

AZ
2025

19. Hackers Red Hat (sombrero rojo)

Los hackers de sombrero rojo (Red Hat Hackers) son defensores digitales que trabajan activamente para proteger sistemas y redes de ataques maliciosos, especialmente contra hackers de sombrero negro (Black Hat). Su función principal es interrumpir y derribar las infraestructuras utilizadas por ciberdelincuentes para causar daño.

Concepto y características

Actúan con métodos ofensivos para detener ataques y desmantelar herramientas y redes de hackers maliciosos.
Son considerados como "guardianes" de la ciberseguridad, combatiendo activamente a los malos actores.
Poseen conocimientos técnicos avanzados en programación, redes, sistemas operativos y criptografía.
Su ética los lleva a respetar la legalidad, privacidad y transparencia, colaborando para fortalecer la seguridad global.
Utilizan tanto habilidades defensivas como ofensivas para neutralizar amenazas antes de que causen daños significativos.

Instrumentos y tecnología digital

Utilizan herramientas de hacking ético y ofensivo, análisis de vulnerabilidades y software especializado para pruebas y ataques controlados.
Emplean técnicas como contramedidas avanzadas, toma de control de sistemas comprometidos por hackers negros y estrategias de defensa activa.
Trabajan con tecnologías de criptografía, sistemas de detección de intrusiones, redes seguras

AZ
2025

19. Hackers Red Hat (sombrero rojo)

Normatividad peruana e internacional

Perú no tiene especificidad legal explícita para hackers Red Hat, pero sus acciones pueden ser encuadradas en la Ley N° 30096 y Código Penal si se realizan dentro de marcos autorizados.

La legislación nacional e internacional promueve la defensa y protección de infraestructuras críticas, contemplando el uso ético de técnicas ofensivas para la ciberdefensa.

El Convenio de Budapest y otros tratados internacionales fomentan la cooperación para la protección del ciberespacio mediante acciones legales, éticas y técnicas.

La regulación distingue claramente el límite entre defensa legítima y actos ilegales sin consentimiento o fuera del marco autorizado.

Sanciones

Las acciones de hackers Red Hat hechas con autorización y para protección no enfrentan sanciones.

Si realizan actividades ofensivas sin marco legal ni consentimiento podrían ser sancionados por la legislación de delitos informáticos.

La normativa peruana y las internacionales buscan equilibrar la flexibilidad en defensa con la protección de derechos y la legalidad.

Sanciones penales, administrativas y técnicas aplican en casos de abuso o acciones ilegales, con énfasis en la prevención y cooperación.

En resumen, los hackers de sombrero rojo son defensores activos que combaten a los ciberdelincuentes con habilidades ofensivas y defensivas, regulados en Perú dentro del marco de delitos informáticos y promovidos internacionalmente para la protección efectiva de sistemas, sin sanciones cuando actúan legalmente.

20. Hackers White Hat (Sombrero Blanco)

AZ
2025

20. Hackers White Hat (Sombrero Blanco)

Los hackers éticos, conocidos como hackers de sombrero blanco (White Hat), son profesionales de la ciberseguridad que utilizan sus habilidades técnicas para detectar vulnerabilidades y proteger sistemas informáticos, siempre actuando con autorización y dentro de la legalidad.

Concepto y características

Actúan para fortalecer la seguridad de redes y sistemas, encontrando fallas antes que los hackers malintencionados (Black Hat).
Su trabajo es preventivo y colaborativo, ayudando a organizaciones públicas y privadas.
Realizan pruebas de penetración, análisis de vulnerabilidades, ingeniería social controlada y creación de sistemas señuelo (honeypots).
Trabajan a partir de un marco ético y legal, con consentimiento para intervenir en sistemas.
Su demanda crece con el aumento de amenazas cibernéticas, siendo esenciales para la ciberdefensa.

Instrumentos y tecnología digital

Usan herramientas de análisis, escaneo de puertos, simulación de ataques y software especializado.
Aplican técnicas avanzadas de hacking ético y forense para evaluar la seguridad.
Utilizan software y equipos para realizar pruebas sin comprometer datos ni funciones críticas.
Pueden participar en programas de recompensa por descubrimiento de errores (bug bounty).

AZ
2025

20. Hackers White Hat (Sombrero Blanco)

Normatividad peruana e internacional

En Perú, la Ley N° 30096 y el Código Penal regulan estas actividades, autorizando el hacking ético con consentimiento.

La legislación promueve la protección de infraestructuras críticas y la ciberseguridad mediante estas prácticas legales.

El Convenio de Budapest y tratados internacionales fomentan la cooperación y el reconocimiento del hacking ético.

El marco legal distingue claramente entre actividades autorizadas y las ilícitas.

Sanciones

Los hackers éticos con autorización no enfrentan sanciones.

Actuar sin consentimiento o provocar daño es sancionable conforme a la ley.

Se fomentan certificaciones y formación para mantener altos estándares éticos y técnicos.

La cooperación internacional refuerza la persecución de ciberdelitos y el soporte a hackers éticos.

En conclusión, los hackers de sombrero blanco son defensores clave en la protección informática, regulados por leyes peruanas e internacionales que los legitiman y sancionan a quienes actúen fuera del marco legal.

21. Hactivistas

AZ
2025

21. Hactivistas

El hacktivismo se define como el uso de técnicas de hacking para promover objetivos políticos, sociales o económicos, generalmente mediante actos de protesta digital que incluyen el acceso no autorizado a sistemas y la interrupción de servicios.

Concepto y características

Los hacktivistas combinan el activismo con el hacking, utilizando ciberataques para apoyar causas ideológicas.
Actúan de manera organizada o individual, con objetivos que van desde la defensa de derechos humanos hasta protestas contra gobiernos o corporaciones.
Generalmente evitan la violencia física, pero sus acciones pueden afectar la disponibilidad, integridad y confidencialidad de sistemas.
En algunos casos, adoptan seudónimos y mantienen anonimato, formando colectivos como "Anonymous".
Su estructura organizativa suele ser horizontal, sin jerarquías estrictas, basada en la confianza y motivación por causas específicas.

Instrumentos y tecnología digital

Utilizan ataques como denegación de servicio (DDoS), defacement (alteración de sitios web), filtración de información y phishing.
Emplean herramientas digitales para acceder a sistemas, difundir mensajes y realizar operaciones coordinadas.
Pueden usar software malicioso dirigido, bots y redes distribuidas para maximizar impacto y alcance.

AZ
2025

21. Hactivistas

Normatividad peruana e internacional

En Perú, el hacktivismo está regulado indirectamente bajo los delitos informáticos en Ley N° 30096 y el Código Penal, especialmente respecto a acceso ilegal a sistemas y daño informático.

No existe una legislación específica que reconozca el hacktivismo como tal, pero sus actos son sancionables según contexto y daños.

A nivel internacional, el hacktivismo es tratado como delito cibernético cuando viola leyes, y está incluido en convenios como el Convenio de Budapest.

La normatividad internacional busca equilibrar la libertad de expresión con la protección de la seguridad y derechos digitales.

Sanciones

Las sanciones en Perú para hacktivistas pueden incluir prisión, multas y medidas de reparación si se comprueba daño, acceso ilegal o fraude.

En casos menos graves, pueden aplicarse sanciones administrativas o medidas preventivas.

Las acciones hacktivistas con consecuencias graves se persiguen con mayor rigor.

Las plataformas digitales suelen tomar medidas técnicas contra estos ataques para proteger la infraestructura y usuarios.

En resumen, los hacktivistas son activistas digitales que usan hacking para promover causas, con un marco normativo en Perú e internacional que sanciona sus actos ilegales, buscando un equilibrio entre derechos y seguridad.

22. Hurtadores informáticos

AZ
2025

22. Hurtadores informáticos

Los hurtadores informáticos son aquellos que cometen el delito de hurto utilizando medios tecnológicos para apropiarse ilegalmente de datos, información, o recursos digitales de otros sin consentimiento.

Concepto y características

Consisten en personas que, mediante acceso no autorizado a sistemas informáticos, redes o dispositivos, sustraen información o bienes digitales.
Actúan con ánimo de lucro, buscando obtener ventaja económica o ventaja competitiva.
Utilizan técnicas de intrusión, robo de credenciales, phishing o malware para fingir acceso legítimo y sustraer información.
Son considerados delincuentes cibernéticos que afectan la propiedad intangible, como datos bancarios, secretos comerciales o información personal.
Pueden operar de forma individual o en grupos organizados, con distintos niveles de sofisticación.

Instrumentos y tecnología digital

Software malicioso: keyloggers, troyanos, ransomware que facilitate la sustracción de datos.
Técnicas de ingeniería social para obtener accesos o contraseñas.
Herramientas de hacking para evadir mecanismos de seguridad.
Plataformas digitales para almacenar o comercializar la información robada.
Redes anónimas para ocultar su identidad y rastros de su actividad.

AZ
2025

22. Hurtadores informáticos

Normatividad peruana e internacional

En Perú, el hurto informático está tipificado y sancionado en la Ley N° 30096 de delitos informáticos y el Código Penal peruano.

Se castigan las conductas que impliquen sustracción, apropiación, acceso ilegal y manipulación de datos o sistemas.

A nivel internacional, normativas como el Convenio de Budapest prevén la persecución de delitos informáticos y protección de la propiedad digital.

Las legislaciones buscan dar respuesta a los nuevos tipos de hurto que afectan derechos digitales y continuidad de servicios.

Sanciones

Las sanciones incluyen penas privativas de libertad, multas y decomiso de bienes relacionados con las actividades ilícitas.

Se agravan en casos de perjuicio a sectores estratégicos, menores o datos sensibles.

Programas de cooperación internacional facilitan la extradición y la investigación conjunta de casos transnacionales.

Se aplica también la confiscación de instrumentos tecnológicos usados para el delito y medidas de reparación a las víctimas.

En resumen, los hurtadores informáticos son ciberdelincuentes especializados en la apropiación ilícita de información y recursos digitales, regulados en Perú e internacionalmente bajo leyes específicas de delitos informáticos con sanciones penales y administrativas para proteger la propiedad digital.

23. Insiders o autores internos

AZ
2025

23. Insiders o autores internos

Los insiders o autores internos son personas con acceso legítimo a la información o sistemas de una organización que, de manera intencional o no, utilizan ese acceso para causar daño, ya sea divulgando información, saboteando sistemas o facilitando ataques externos.

Concepto y características

Son empleados, exempleados, contratistas o socios comerciales con acceso autorizado a recursos internos.
Pueden actuar de forma maliciosa, buscando lucro o venganza, o de forma negligente por errores o falta de conocimiento.
Los daños que pueden causar incluyen fuga de información sensible, sabotaje, alteración de datos o facilidades para ataques externos.
Presentan un riesgo significativo porque los sistemas de seguridad tradicionales no detectan fácilmente actividades internas maliciosas.
La amenaza de insiders es creciente y representa un porcentaje importante de los incidentes de seguridad en empresas.

Instrumentos y tecnología digital

Uso indebido de credenciales, acceso a datos sensibles y sistemas de control interno.
Instalación o uso de malware y herramientas para extracción de datos.
Redes sociales y comunicación interna para coordinar actos maliciosos.
Uso de dispositivos personales o remotos para acceder y filtrar información.
Realizan acciones que aprovechan vulnerabilidades humanas antes que técnicas.

AZ
2025

23. Insiders o autores internos

Normatividad peruana e internacional

En Perú, la Ley N° 30096 y el Código Penal sancionan el uso indebido de acceso a sistemas y datos, incluyendo a insiders.

Se tipifican delitos como acceso ilícito, difusión de información confidencial, sabotaje digital y fraude.

Normas internacionales, como el Convenio de Budapest, reconocen la amenaza de insiders y promueven políticas de seguridad integrales.

La normatividad exige a organizaciones implementar controles de acceso, monitoreo y medidas de respuesta a amenazas internas.

Sanciones

Las sanciones pueden incluir cárcel, multas y responsabilidad civil cuando insiders causan daño o facilitan delitos informáticos.

Se agravan las penas si los actos afectan a sectores estratégicos o involucran información sensible.

Las empresas también pueden aplicar sanciones disciplinarias y contratos de confidencialidad para prevenir riesgos.

La cooperación internacional facilita la investigación y persecución de estos delitos que trascienden fronteras.

En síntesis, los insiders son amenazas internas con acceso a recursos de la organización que pueden poner en riesgo la seguridad mediante acciones maliciosas o negligentes. Están regulados en Perú y a nivel internacional con sanciones penales y civiles para proteger la integridad de la información y sistemas.

24. Ladrones informáticos

AZ
2025

24. Ladrones informáticos

Los ladrones informáticos son delincuentes que utilizan medios tecnológicos para cometer actos ilícitos de apropiación ilegal de información, recursos digitales o activos económicos mediante sistemas informáticos.

Concepto y características

Cometen delitos a través de la manipulación, acceso no autorizado o robo de datos y recursos digitales, como información personal, bancaria o patrimonial.
Son expertos en explotar vulnerabilidades de sistemas y redes, actuando a distancia sin necesidad de presencia física.
Sus acciones provocan pérdidas financieras significativas y afectan la integridad, confidencialidad y disponibilidad de la información.
Operan con sofisticación técnica, utilizando malware, phishing, ransomware, ataques de denegación de servicio, y fraudes electrónicos.
Esta actividad es realizada tanto por individuos como por grupos organizados a nivel local e internacional.

Instrumentos y tecnología digital

Utilizan software malicioso (virus, troyanos) para infiltrarse y robar información.
Emplean técnicas de ingeniería social y phishing para obtener credenciales y acceso ilegal.
Ransomware para secuestrar información digital y exigir rescate.
Plataformas de intercambio anónimas y criptomonedas para ocultar flujos ilícitos.
Redes de bots para amplificar ataques y dificultar la detección.

AZ
2025

24. Ladrones informáticos

Normatividad peruana e internacional

En Perú, la Ley N° 30096 y el Código Penal sancionan conductas de hurto, fraude, acceso no autorizado y daño informático.

El marco jurídico contempla delitos de robo informático, fraude electrónico, y otros relacionados con hurtos en sistemas digitales.

A nivel internacional, tratados como el Convenio de Budapest establecen medidas para prevenir, investigar y castigar delitos informáticos transnacionales.

Las normativas buscan proteger a usuarios, empresas e infraestructuras críticas, promoviendo cooperación internacional.

Sanciones

Penas privativas de libertad, multas y decomiso de bienes para responsables de delitos de robo digital.

Agravantes en casos que afecten sistemas estratégicos, datos sensibles o causen daños graves.

Medidas preventivas, técnicas y legales para limitar la acción de ladrones informáticos.

Colaboración judicial internacional para persecución y extradición de delincuentes cibernéticos.

En resumen, los ladrones informáticos son sujetos que cometen hurtos y fraudes mediante el uso de tecnologías digitales, regulados y sancionados en el Perú y en la legislación internacional con un enfoque en protección, prevención y persecución del delito informático.

25. Malwaristas

AZ
2025

25. Malwaristas

Los malwaristas son ciberdelincuentes especializados en la creación, distribución y uso malicioso de malware, que son programas diseñados para infiltrarse, dañar o tomar control de sistemas informáticos sin el consentimiento de los usuarios.

Concepto y características

Se dedican a crear y propagar software malicioso como virus, troyanos, ransomware, spyware, gusanos, entre otros.
Sus objetivos incluyen robar información, extorsionar, causar daños, generar interrupciones o espionaje.
Operan en ámbitos clandestinos, usando técnicas avanzadas para evadir detección y análisis forense.
Trabajan solitarios o en grupos organizados, a menudo asociados con otras formas de ciberdelincuencia.
Su actividad es sofisticada, con actualizaciones constantes para superar defensas y adaptarse a nuevas tecnologías.

Instrumentos y tecnología digital

Desarrollo y uso de malware específico para diferentes objetivos (robo de datos, control remoto, extorsión).
Plataformas de distribución como correos electrónicos, redes sociales, sitios web comprometidos y programas pirata.
Criptomonedas para monetizar ataques y facilitar el lavado de dinero.
Redes de bots (botnets) para ataques masivos y control remoto de múltiples computadores

AZ
2025

25. Malwaristas

Normatividad peruana e internacional

En Perú, la Ley N° 30096 sobre delitos informáticos tipifica y sanciona la creación, distribución y uso de malware.

El Código Penal complementa con penas por daño informático, acceso ilícito, fraude y otros delitos relacionados.

A nivel internacional, el Convenio de Budapest regula la cooperación para prevenir y sancionar delitos informáticos vinculados con malware.

La normativa busca proteger la integridad, confidencialidad y disponibilidad de sistemas, así como a los usuarios afectados.

Sanciones

Penas de prisión privativa, multas elevadas y decomiso de equipos y bienes relacionados con actividades de malware.

Agravantes si afectan infraestructuras críticas, servicios públicos, usuarios vulnerables o menores.

Medidas técnicas y legales para bloquear, neutralizar y prevenir ataques, además de mecanismos de cooperación internacional.

Políticas de ciberseguridad que incluyen capacitación, detección temprana y respuesta rápida frente a ataques de malware.

En conclusión, los malwaristas son delincuentes especializados que usan software malicioso para atacar sistemas y lograr fines ilícitos, regulados en Perú y en normativas internacionales con sanciones severas para proteger la seguridad digital y la integridad de la información.

.

26. Pharming

AZ
2025

26. Pharming

El pharming es una técnica de ciberdelincuencia que consiste en redirigir de forma fraudulenta el tráfico de usuarios desde un sitio web legítimo hacia uno falso, con el objetivo de capturar información personal, financiera o confidencial sin que el usuario se percate del engaño.

Concepto y características

El pharming manipula la resolución de nombres de dominio (DNS) o archivos de hosts en computadoras para redirigir a los usuarios a sitios web fraudulentos idénticos a los originales.
A diferencia del phishing, que utiliza correos fraudulentos o mensajes para engañar a la víctima, el pharming puede afectar a múltiples usuarios independientemente de la interacción con mensajes.
Es más complejo y difícil de detectar para el usuario, pues la redirección ocurre sin su conocimiento al escribir una URL correcta.
Busca el robo de datos sensibles, como credenciales bancarias, números de tarjetas de crédito o información personal.
Puede afectar redes o sistemas enteros mediante el envenenamiento de la caché DNS o ataques a servidores DNS.

Instrumentos y tecnología digital

Manipulación de servidores DNS para alterar la ruta de navegación.
Modificación de archivos de hosts locales en dispositivos de víctimas.
Uso de malware que modifica configuraciones de red para redireccionar tráfico.
Creación de sitios web falsos, idénticos en apariencia a los legítimos para engañar.

AZ
2025

26. Pharming

Normatividad peruana e internacional

En Perú, el pharming es considerado un delito informático contemplado en la Ley N° 30096 y el Código Penal, por el acceso ilegal y manipulación de sistemas que provoca daño a terceros.
Se sanciona la manipulación de sistemas de red, la suplantación de identidad y el robo de información bajo estos marcos legales.
A nivel internacional, el Convenio de Budapest y otras normativas contienen directrices para combatir estas amenazas mediante cooperación y sanciones.
La legislación busca proteger la infraestructura crítica de internet y garantizar la seguridad y confianza en el entorno digital.

Sanciones

Incluyen penas de prisión, multas y decomiso de equipos y recursos informáticos usados en ataques.
Aggravantes cuando afectan servicios esenciales, minorías o causan daños significativos.
Se aplican medidas técnicas para bloquear y mitigar ataques y proteger a los usuarios.
La cooperación judicial internacional es clave para perseguir a los responsables en el ámbito transnacional.
En suma, el pharming es un ataque avanzado que redirige usuarios a sitios falsos para robar datos, regulado en Perú mediante leyes contra delitos informáticos y en normativas internacionales con sanciones penales para proteger la integridad del ciberespacio.

27. Phising digitales (pescadores)

AZ
2025

27. Phising digitales (pescadores)

El phishing digital, también conocido como "pescadores" en un sentido figurado, es una técnica de ciberdelincuencia que consiste en engañar a las personas para que entreguen información sensible mediante el uso de correos electrónicos, mensajes o sitios web falsos que simulan ser de fuentes confiables.

Concepto y características

Los atacantes se hacen pasar por entidades legítimas, como bancos, plataformas digitales o empresas reconocidas, para robar datos personales, contraseñas o información financiera.
Utilizan correos electrónicos fraudulentos, mensajes de texto, mensajes en redes sociales o llamadas telefónicas para persuadir a la víctima.
Los mensajes suelen contener enlaces a sitios falsos o archivos adjuntos maliciosos que infectan el dispositivo con malware.
El phishing puede ser genérico (enviado en masa) o dirigido (spear phishing), con mensajes personalizados basados en información previa.
Entre sus variantes están el smishing (a través de SMS) y el vishing (con llamadas telefónicas).

Instrumentos y tecnología digital

Enlaces maliciosos que redirigen a páginas fraudulentas.
Archivos adjuntos con malware o virus.
Formularios falsos para capturar datos personales.
Técnicas de ingeniería social para manipular conductas.
Software de seguimiento para capturar credenciales y datos.

AZ
2025

27. Phising digitales (pescadores)

Normatividad peruana e internacional

En Perú, el phishing está tipificado dentro de la Ley N° 30096 y el Código Penal que sancionan el acceso indebido, fraude y robo de identidad.

La legislación protege la información personal y prohíbe la suplantación de identidad mediante medios digitales.

A nivel internacional, el Convenio de Budapest y otras normativas buscan prevenir, investigar y sancionar estas prácticas.

La normativa promueve la educación y medidas de seguridad para reducir la efectividad del phishing.

Sanciones

Penas de prisión, multas y decomiso de bienes para quienes cometan phishing con fines ilícitos.

Se agravan las sanciones cuando involucran datos sensibles, menores o afectan a instituciones públicas.

Las sanciones incluyen medidas técnicas para bloquear el acceso a sitios fraudulentos y proteger a las víctimas.

La cooperación internacional es fundamental para enfrentar esta amenaza transnacional.

En resumen, el phishing digital es un método de engaño para robar información usando suplantación y mensajes falsos, regulado en Perú y a nivel internacional con sanciones para proteger a los usuarios y la integridad de la información digital.

28. Piratas digitales

AZ
2025

28. Piratas digitales

Los piratas digitales, también conocidos como hackers o ciberdelincuentes, son personas que utilizan medios tecnológicos para acceder de manera no autorizada a sistemas informáticos, redes o datos, con el fin de causar daño, robar información o obtener beneficios ilícitos.

Concepto y características

Se dedican a actividades ilegales como el acceso no autorizado, robo de datos, sabotaje, fraude y espionaje digital.
Operan con diversas motivaciones, incluyendo lucro económico, espionaje corporativo, notoriedad o fines políticos.
Emplean técnicas sofisticadas para vulnerar la seguridad de sistemas y mantener el anonimato.
Pueden ser individuos solitarios, grupos organizados o estar patrocinados por estados.
Su actividad genera graves impactos en la privacidad, economía y seguridad de individuos, empresas y gobiernos.

Instrumentos y tecnología digital

Utilizan malware (virus, troyanos, ransomware), phishing, ataques de denegación de servicio y explotación de vulnerabilidades.
Emplean métodos de ingeniería social para engañar usuarios y obtener acceso.
Usan redes clandestinas y herramientas para ocultar su identidad y rastros.
Operan en la dark web y otros espacios digitales poco regulados para coordinar actividades.

AZ
2025

28. Piratas digitales

Normatividad peruana e internacional

En Perú, la Ley N° 30096 y el Código Penal regulan y sancionan el acceso ilícito, daño informático, fraude y otros delitos cibernéticos.

A nivel internacional, el Convenio de Budapest y otros acuerdos facilitan la cooperación para combatir la piratería digital y otros delitos informáticos.

La legislación busca proteger infraestructuras críticas, derechos digitales y promover la seguridad cibernética.

Existen marcos legales que diferencian entre actividades legales (hacking ético) y actos criminales.

Sanciones

Penas de prisión, multas y decomiso de activos para quienes cometen delitos de piratería informática.

Agravantes en casos de impacto a sectores estratégicos, menores o datos sensibles.

Medidas judiciales y técnicas para mitigar ataques y proteger a las víctimas.

Cooperación internacional para la captura y procesamiento de piratas digitales.

En conclusión, los piratas digitales son actores que cometen delitos informáticos con diversas motivaciones y técnicas, regulados en Perú y globalmente con sanciones penales y administrativas destinadas a proteger la seguridad y la integridad del ciberespacio.

29. Qrshing

AZ
2025

29. Qrshing

El QRshing es una modalidad de phishing que utiliza códigos QR fraudulentos para engañar a los usuarios y hacer que revelen información personal, financiera o confidencial al ser dirigidos a sitios web falsos o al descargar malware en sus dispositivos.

Concepto y características

Se basa en la manipulación o creación de códigos QR que, al ser escaneados, redirigen a sitios web falsos o activan descargas maliciosas.

Los atacantes aprovechan la confianza en los códigos QR para distribuir enlaces peligrosos de forma rápida y masiva.

Es difícil para el usuario detectar la amenaza, ya que los códigos QR no muestran la URL antes de interactuar.

Puede afectar desde usuarios individuales hasta empresas, facilitando robos de datos bancarios, credenciales y otros fraudes.

El QRshing se ha incrementado con el uso creciente de códigos QR en pagos, accesos y registros digitales.

Instrumentos y tecnología digital

Generadores de códigos QR falsos con enlaces maliciosos.

Páginas web clonadas o fraudulentas para capturar datos o instalar malware.

Malware que se activa al escanear o interactuar con el código.

Técnicas de ingeniería social para inducir al usuario a escanear el código.

AZ
2025

29. Qrshing

Normatividad peruana e internacional

En Perú, el QRshing se enmarca dentro de los delitos informáticos sancionados por la Ley N° 30096 y el Código Penal, tipificando fraudes, accesos ilícitos y manipulación de sistemas digitales.

A nivel internacional, está incluido en la regulación general sobre delitos cibernéticos y fraudes electrónicos, como en el Convenio de Budapest.

La legislación busca proteger la confidencialidad, integridad y seguridad de la información y los sistemas digitales.

Fomenta campañas de prevención y educación sobre el uso seguro de tecnologías digitales.

Sanciones

Penas de prisión, multas y decomiso de equipos usados en ataques de QRshing.

Agravadas cuando afectan servicios críticos, menores o generan daños económicos significativos.

Medidas técnicas para bloquear sitios fraudulentos y alertar a usuarios.

Cooperación internacional para la investigación y captura de responsables.

En resumen, el QRshing es un tipo de phishing que usa códigos QR falsos para engañar y robar datos, regulado en Perú e internacionalmente con sanciones severas para proteger a usuarios y sistemas digitales.

31. Ransowares (secuestradores digitales)

AZ
2025

31. Ransowares (secuestradores digitales)

Los ransomwares, conocidos como secuestradores digitales, son un tipo de malware diseñado para cifrar o bloquear el acceso a los datos o sistemas de una víctima, solicitando un rescate económico para liberar esa información o recuperar el control del sistema.

Concepto y características

El ransomware cifra archivos o bloquea el acceso a dispositivos hasta que se pague un rescate, generalmente en criptomonedas para mantener el anonimato.
Puede afectar tanto a individuos como a empresas o instituciones, causando interrupciones significativas y pérdidas económicas.
Las variantes modernas incluyen la doble extorsión, donde además de cifrar, se amenazan con divulgar la información robada.
Su distribución se da por correos phishing, exploiting de vulnerabilidades, accesos remotos comprometidos, o descargas de software malicioso.
Es uno de los ataques más peligrosos y con crecimiento exponencial en el ámbito de la ciberseguridad.

Instrumentos y tecnología digital

Malware específico que cifra archivos y controla sistemas, extorsionando a la víctima.
Plataformas de pago anónimas como Bitcoin para recibir rescates.
Campañas de phishing y exploit kits para distribución.
Redes de bots (botnets) para amplificación y propagación.
Herramientas para evadir detección y mantener persistencia.

AZ
2025

31. Ransowares (secuestradores digitales)

Normatividad peruana e internacional

Perú regula el ransomware en la Ley N° 30096 sobre delitos informáticos y el Código Penal, donde se sanciona el acceso ilícito, daño informático y extorsión.

Se aprobó el Reglamento de la Ley de Ciberdefensa (Decreto Supremo N° 017-2024-PCM) para proteger los activos críticos y garantizar la seguridad nacional frente a estos ataques.

El Convenio de Budapest y otros tratados internacionales promueven la cooperación en la prevención y persecución del ransomware a nivel global.

La normativa peruana enfatiza la protección de infraestructuras esenciales y la continuidad de servicios ante ataques cibernéticos.

Sanciones

Las penas incluyen prisión efectiva, multas y decomiso de bienes relacionados con la ejecución o apoyo de ataques ransomware.

Sanciones más severas si se afectan infraestructuras críticas o datos sensibles.

Se incluyen medidas técnicas y jurídicas para bloqueo de ataques, recuperación y protección.

La cooperación internacional es esencial para la investigación y captura de los responsables.

En conclusión, los ransomwares (secuestradores digitales) son malware que extorsionan cifrando datos, regulados severamente en Perú e internacionalmente para proteger la seguridad y estabilidad digital, con sanciones penales y medidas de defensa especificas.

32. Saboteadores digitales

AZ
2025

32. Saboteadores digitales

Los saboteadores digitales son personas o agentes que realizan acciones maliciosas para afectar, interrumpir o destruir el funcionamiento normal de sistemas, redes o información digital, causando daños que pueden ir desde pérdida temporal de servicio hasta consecuencias económicas graves.

Concepto y características

El sabotaje digital consiste en la alteración, destrucción o modificación sin autorización de datos, programas o infraestructura tecnológica con la intención de causar perjuicio.
Puede manifestarse como eliminación de archivos, bloqueo de sistemas, implantación de virus, gusanos o bombas lógicas.
Son acciones deliberadas para obstaculizar operaciones normales, afectar la integridad y disponibilidad de información.
Los saboteadores pueden ser internos (empleados descontentos) o externos (ciberdelincuentes, estados).
Presentan alto riesgo para organizaciones, especialmente aquellas con dependencia crítica en sus sistemas tecnológicos.

Instrumentos y tecnología digital

Virus, gusanos, troyanos, bombas lógicas y otros tipos de malware con capacidad destructiva.
Técnicas de ingeniería social para obtener accesos no autorizados y ejecutar sabotajes.
Modificación o eliminación de respaldos para dificultar la recuperación.
Accesos remotos maliciosos y explotación de vulnerabilidades.
Uso de sistemas para alterar configuraciones, bloqueos o destrucción de datos.

AZ
2025

32. Saboteadores digitales

Normatividad peruana e internacional

En Perú, el sabotaje informático está tipificado en el artículo 264 del Código Penal y regulado en la Ley N° 30096 de delitos informáticos.

Se sancionan las conductas que dañan, inutilizan o alteran sistemas y datos ajenos sin autorización.

A nivel internacional, el Convenio de Budapest incluye esta figura dentro de los delitos informáticos para promover cooperación.

La legislación busca proteger servicios esenciales, infraestructura crítica y los derechos digitales.

Sanciones

Penas de prisión de 6 meses a 3 años, que pueden aumentar hasta 5 años en casos graves o grupales.

Multas económicas y decomiso de instrumentos utilizados para el sabotaje.

Medidas compensatorias y técnicas para restablecer y proteger sistemas afectados.

Responsabilidad penal reforzada si se afectan sectores estratégicos o se causan daños significativos.

En resumen, los saboteadores digitales realizan actos dañinos contra sistemas informáticos con graves consecuencias, regulados y sancionados en Perú y mundialmente bajo legislaciones que protegen la integridad y continuidad de sistemas digitales.

33. Script Kiddies

AZ
2025

33. Script Kiddies

Los Script Kiddies son individuos, generalmente jóvenes o inexpertos en ciberseguridad, que utilizan herramientas, scripts y programas desarrollados por hackers expertos para llevar a cabo ataques informáticos sin comprender completamente cómo funcionan esas herramientas o las consecuencias de sus acciones.

Concepto y características

No poseen habilidades técnicas avanzadas ni capacidad para crear sus propios exploits.
Suelen atacar para impresionar a sus pares o ganar notoriedad en comunidades online.
Utilizan herramientas públicas o fácilmente accesibles para realizar ataques básicos.
Cometen acciones como ataques de denegación de servicio (DoS), defacement de sitios, phishing básico y otras actividades con impacto limitado pero potencialmente dañino.
Su falta de conocimientos suele dejar rastros que facilitan su detección y seguimiento.

Instrumentos y tecnología digital

Scripts y software preexistente para explotación de vulnerabilidades.
Usan técnicas de ingeniería social sencillas para obtener información.
Herramientas accesibles para ataques automatizados o semi-automatizados.
Plataformas y foros donde descargan y comparten recursos para atacar.

AZ
2025

33. Script Kiddies

Normatividad peruana e internacional

En Perú, sus actos son regulados por la Ley N° 30096 y el Código Penal bajo normas que sancionan el acceso ilegal, daño informático, fraudes y otros delitos cibernéticos.

La legislación busca sancionar incluso los ataques de bajo nivel a fin de proteger sistemas e información.

A nivel internacional, el Convenio de Budapest y otras regulaciones establecen marcos para perseguir cualquier tipo de ataque informático, independientemente del nivel técnico.

Se promueve la educación y formación para prevenir estas conductas.

Sanciones

Penas de prisión y multas aplican para quienes efectúan ataques, incluso si son cometidos por inexpertos.

Se agravan las penas si causan daños significativos, afectan servicios críticos o a menores.

Las sanciones incluyen decomiso de equipos y medidas restaurativas.

La cooperación internacional ayuda a identificar y sancionar a los responsables.

En resumen, los Script Kiddies son atacantes inexpertos que emplean herramientas de terceros para realizar ataques informáticos, regulados y sancionados en Perú e internacionalmente para proteger la seguridad digital frente a todas las formas de intrusión.

34. Sim Swapping

AZ
2025

34. Sim Swapping

El SIM swapping, también conocido como secuestro de SIM, es un fraude en el que los ciberdelincuentes duplican de forma fraudulenta la tarjeta SIM de la víctima para tomar el control de su número de teléfono, con el fin de acceder a su información personal y cuentas digitales, incluyendo banca en línea y redes sociales.

Concepto y características

El atacante obtiene datos personales de la víctima (DNI, contraseñas, etc.) mediante ingeniería social, phishing o análisis de redes sociales.
Contacta a la operadora de telefonía móvil haciéndose pasar por la víctima para que transfiera el número a una nueva SIM en su poder.
La víctima pierde el servicio telefónico y el atacante recibe todos los SMS y llamadas, incluyendo códigos de autenticación de dos factores.
Es un método sofisticado para evadir medidas de seguridad y robar identidades, dinero y datos.
Puede involucrar la complicidad de empleados de compañías telefónicas o uso de redes wifi falsas y aplicaciones maliciosas.

Instrumentos y tecnología digital

Ingeniería social para recolectar información.
Comunicación con operadores telefónicos mediante llamadas o presencialmente.
Software malicioso para espiar y captar datos personales.
Redes y aplicaciones para ocultar actividades y controlar el dispositivo.

AZ
2025

34. Sim Swapping

Normatividad peruana e internacional

En Perú, el SIM swapping está tipificado dentro de la Ley N° 30096 y el Código Penal, bajo delitos informáticos relacionados con la suplantación, fraude y acceso ilegal.

Se considera delito grave por la afectación a la privacidad y seguridad financiera de las personas.

A nivel internacional, está contemplado en el Convenio de Budapest y otros tratados contra la ciberdelincuencia.

Normativas promueven medidas para proteger a los usuarios y penalizar a los responsables.

Sanciones

Penas de prisión, multas y confiscación de bienes para quienes cometen SIM swapping.

Se aplican sanciones agravadas si afectan infraestructuras críticas o datos sensibles.

Se implementan mecanismos de control y monitoreo en operadoras para evitar fraudes.

La cooperación internacional ayuda a perseguir a delincuentes en diferentes jurisdicciones.

En síntesis, el SIM swapping es un delito informático serio que permite el secuestro digital del número telefónico para cometer fraudes, regulado y sancionado en Perú e internacionalmente con medidas legales y técnicas para la protección de los usuarios.

35. Smishing

AZ
2025

35. Smishing

El smishing es una modalidad de ciberdelito que consiste en realizar ataques de phishing a través de mensajes SMS o de texto, utilizando técnicas de ingeniería social para engañar a las víctimas y obtener información confidencial, financiera o instalaciones de malware en sus dispositivos.

Concepto y características

Es una combinación de “SMS” y “phishing”, donde los atacantes envían mensajes de texto falsos que parecen legítimos.

Los mensajes suelen generar urgencia, miedo o curiosidad para inducir a la víctima a hacer clic en enlaces, responder con información privada o descargar archivos maliciosos.

Los mensajes pueden aparecer como provenientes de bancos, empresas, instituciones oficiales, amigos o familiares.

El objetivo principal es robar credenciales, información personal, datos bancarios o inducir a transferencias fraudulentas.

Puede incluir variantes que usan plataformas de mensajería basadas en datos, como WhatsApp.

Instrumentos y tecnología digital

Mensajes SMS con enlaces a sitios web falsos o archivos adjuntos.

Páginas de captura fraudulentas para robar información.

Malware oculto en archivos o vinculaciones que infectan dispositivos.

Técnicas de suplantación para mostrar remitentes confiables.

Herramientas que permiten envío masivo de mensajes y manipulación de identidad digital

AZ
2025

35. Smishing

Normatividad peruana e internacional

En Perú, el smishing está regulado bajo la Ley N° 30096 y el Código Penal, que sancionan la suplantación de identidad, fraude y acceso ilegal a datos.

La normativa protege a los usuarios de telecomunicaciones y la integridad de la información personal.

A nivel internacional, el Convenio de Budapest y otros acuerdos promueven la cooperación para combatir estos delitos.

Las leyes fomentan la educación y concienciación para prevenir víctimas de smishing.

Sanciones

Incluyen penas privativas de libertad, multas y decomiso de equipos usados en los ataques.

Agravantes cuando los ataques afectan a menores, provocan daños económicos o afectan servicios esenciales.

Medidas técnicas para bloquear mensajes fraudulentos y proteger a usuarios.

Colaboración internacional para identificar y sancionar a los responsables.

En conclusión, el smishing es un peligroso ataque a través de mensajes SMS que busca engañar y robar datos, con regulación y sanciones en Perú y el ámbito internacional para proteger la seguridad digital y personal de los usuarios.

36. Sock puppets (Tìteres digitales

AZ
2025

36. Sock puppets (Tìteres digitales

Los "Sock Puppets" o títeres digitales son perfiles o identidades falsas creados en plataformas digitales y redes sociales, manipulados generalmente por una persona o grupo con el objetivo de influir en conversaciones, opiniones o percepciones públicas sin revelar la verdadera identidad del autor.

Concepto y características

Son cuentas o perfiles falsos creados para simular usuarios reales.
Usados para manipular debates, inflar apoyo a opiniones propias, difundir desinformación o acosar a terceros de forma encubierta.
Pueden actuar coordinadamente para amplificar mensajes o crear falsas consensos.
Su actividad suele ser difícil de detectar por la apariencia legítima de los perfiles.
Se emplean en campañas de desinformación, marketing engañoso, y manipulación política o social.

Instrumentos y tecnología digital

Uso de múltiples cuentas en redes sociales, foros o plataformas de comentarios.
Software para automatizar publicaciones y respuestas (bots).
Técnicas para ocultar direcciones IP y evitar rastreo.
Creación de identidades falsas con imágenes, nombres y datos fabricados.
Herramientas para coordinar acciones sincronizadas y masivas.

AZ
2025

36. Sock puppets (Tìteres digitales

Normatividad peruana e internacional

En Perú, estas prácticas pueden estar tipificadas como delitos de suplantación de identidad, acoso digital, difamación y manipulación fraudulenta en la Ley N° 30096 y el Código Penal.

A nivel internacional, la regulación incluye normativas contra la difusión de noticias falsas, fraude y delitos digitales.

La legislación busca proteger la integridad informativa, los derechos digitales y la privacidad.

Se promueve la transparencia y la responsabilidad en el uso de plataformas digitales.

Sanciones

Penas de prisión, multas y bloqueos de cuentas para quienes crean y operan sock puppets con fines ilegales.

Agravación de sanciones en casos de daño reputacional, acoso sistemático o afectación a instituciones.

Medidas técnicas para detectar y eliminar perfiles falsos y proteger a las víctimas.

Cooperación internacional para enfrentar redes de desinformación y manipulación.

En conclusión, los sock puppets o títeres digitales son identidades falsas utilizadas para manipular y ocultar la verdad en entornos digitales, regulados en Perú y globalmente con sanciones para proteger la verdad, la privacidad y la seguridad en el ciberespacio.

37. Spear Phishing

AZ
2025

37. Spear Phishing

El spear phishing es una modalidad sofisticada de phishing dirigida específicamente a una persona, grupo u organización determinado. A diferencia del phishing común (masivo y genérico), el spear phishing utiliza información personalizada y técnicas de ingeniería social para engañar a la víctima de manera más efectiva.

Concepto y características

Es un ataque selectivo y personalizado que busca obtener información sensible o acceso a sistemas privados.
Los atacantes investigan a fondo a sus objetivos usando redes sociales, bases de datos y otras fuentes para adaptar los mensajes.
Los correos o mensajes aparentan proceder de fuentes confiables como colegas, jefes, bancos o instituciones.
Pueden incluir estafas para descargar malware, divulgar información o transferir fondos.
Es altamente efectivo porque explota la confianza y vulnerabilidades humanas con mensajes convincentes y dirigidos.

Instrumentos y tecnología digital

Correos electrónicos, mensajes en redes sociales, SMS o llamadas telefónicas personalizados.
Técnicas de ingeniería social para crear escenarios verosímiles y ganar la confianza de la víctima.
Páginas web falsificadas para capturar datos o distribuir malware.
Software para automatizar la recopilación de información y envío dirigido.
Incorporación de avances tecnológicos como IA para crear mensajes y voces deepfake más

AZ
2025

37. Spear Phishing

Normatividad peruana e internacional

En Perú, el spear phishing está regulado en la Ley N° 30096 y el Código Penal, que sancionan delitos de suplantación de identidad, acceso ilegal y fraude informático.

La legislación protege a personas y organizaciones contra estos ataques mediante normas que regulan la integridad y seguridad informática.

Internacionalmente, el Convenio de Budapest y otras regulaciones abordan estos delitos con énfasis en la cooperación para la investigación y sanción.

Se fomenta la conciencia y capacitación para que empresas y usuarios detecten y prevengan estos ataques.

Sanciones

Penas de prisión, multas y decomisos para responsables de ataques de spear phishing.

Agravantes en casos que afecten sectores estratégicos, causen daños económicos o involucren a menores.

Medidas técnicas y judiciales para mitigar ataques, proteger víctimas y desmantelar redes criminales.

Colaboración internacional para la persecución y condena de los perpetradores.

En resumen, el spear phishing es una modalidad altamente personalizada y peligrosa de phishing, regulada en Perú y globalmente, con sanciones y medidas que buscan proteger la seguridad digital e información confidencial de personas y organizaciones.

38. Spyware

AZ
2025

38. Spyware

El spyware es un software malicioso que se instala en un dispositivo sin el conocimiento o consentimiento del usuario para espiar su actividad y recolectar información confidencial, transmitiéndola a terceros con fines ilícitos o comerciales.

Concepto y características

El spyware monitorea la actividad del usuario, captura contraseñas, datos bancarios, hábitos de navegación y otra información sensible.
Funciona de manera oculta, ejecutándose en segundo plano y dificultando su detección.
Puede ralentizar el rendimiento del dispositivo al consumir recursos como memoria (RAM) y procesamiento.
Su instalación suele ocurrir a través de descargas engañosas, sitios web maliciosos, correos electrónicos o software adjunto.
Se considera una grave amenaza contra la privacidad y la seguridad digital, con posibles consecuencias como robo de identidad y pérdidas financieras.

Instrumentos y tecnología digital

Incluye spyware troyano, adware, cookies de rastreo y supervisores de sistema.
Técnicas de ocultamiento para evitar la detección por antivirus.
Herramientas para recopilar y transmitir datos sin consentimiento.
Puede instalar software adicional para aumentar el control del atacante.
Utiliza vectores comunes de infección como enlaces maliciosos y archivos adjuntos.

AZ
2025

38. Spyware

Normatividad peruana e internacional

En Perú, el spyware está regulado en la Ley N° 30096 y el Código Penal que sancionan el acceso ilícito, interceptación y uso no autorizado de información.

La legislación protege la privacidad, integridad y confidencialidad de datos personales y corporativos.

Internacionalmente, el Convenio de Budapest y otros tratados establecen marcos para la persecución del uso y distribución de software espía.

Se impulsa la educación y adopción de tecnologías para prevención y detección.

Sanciones

Incluyen penas de prisión, multas y medidas cautelares para detener la distribución y uso del spyware.

Se agravan en casos de afectación a infraestructuras críticas, datos sensibles o grupos vulnerables.

Se aplican medidas técnicas de protección, monitoreo y respuesta ante infecciones.

La cooperación internacional es vital para desmantelar redes de spyware y perseguir a los atacantes.

En conclusión, el spyware es un software malicioso que compromete la privacidad y seguridad de los usuarios, regulado en Perú e internacionalmente con sanciones destinadas a proteger los sistemas y datos digitales de amenazas encubiertas.

39. Troyanos

AZ
2025

39. Troyanos

Los troyanos, también conocidos como caballos de Troya, son un tipo de malware que se disfraza de programa legítimo para engañar al usuario y lograr la instalación en su sistema sin ser detectado. Una vez activo, permite a los atacantes acceder, controlar o robar información del dispositivo infectado.

Concepto y características

Se presentan como software inofensivo para inducir al usuario a ejecutarlos o instalarlos.
No se autorreplican como los virus, sino que se propagan mediante engaños y técnicas de ingeniería social.
Pueden crear puertas traseras (backdoors) para que atacantes accedan remotamente.
Son capaces de espiar la actividad, robar datos, controlar dispositivos, instalar otros malware y lanzar ataques.
Suelen componerse de dos programas: uno que controla desde el atacante y otro residente en el equipo infectado.

Instrumentos y tecnología digital

Archivos adjuntos en correos electrónicos, programas gratuitos o enlaces falsos.
Herramientas que permiten accesos directos o inversos para comunicación con el atacante.
Técnicas para ocultarse en el sistema y evadir antivirus.
Posibilidad de modificar el software residente mediante editores protegidos.
Emplean puertos personalizados para la conexión remota.

AZ
2025

39. Troyanos

Normatividad peruana e internacional

En Perú, el uso y distribución de troyanos está tipificado en la Ley N° 30096 de delitos informáticos y el Código Penal.

La legislación penaliza el acceso ilegal, daño informático, espionaje y robo de información mediante estos programas.

En el ámbito internacional, el Convenio de Budapest y otras normas cooperan para tipificar y perseguir estos delitos.

Se fomenta la educación y el desarrollo de tecnologías de defensa para contrarrestar la amenaza.

Sanciones

Penas de prisión y multas a quienes desarrollen, distribuyan o utilicen troyanos con fines maliciosos.

Agravación en casos que involucren daño a infraestructuras críticas o datos sensibles.

Medidas técnicas para la detección y eliminación de troyanos, así como restauración de sistemas.

Colaboración internacional para la investigación y captura de responsables.

En resumen, los troyanos son malware que se ocultan en softwares aparentes para permitir accesos no autorizados y robos de información, regulados y sancionados en Perú y globalmente con leyes diseñadas para proteger la integridad y la seguridad en el ciberespacio.

40. Viejoverdes digitales (**grooming**)

AZ
2025

40. Viejoverdes digitales

El término "viejoverdes digitales" no es un concepto formalmente definido en normativas peruanas ni internacionales ni en literatura técnica sobre ciberdelincuencia o tecnología digital. Sin embargo, el término "viejo verde" tiene una connotación social y cultural bien reconocida que se refiere a una persona mayor que muestra un interés sexual inapropiado hacia personas notablemente más jóvenes, y esta idea puede trasladarse al contexto digital para referirse a personas mayores que utilizan las plataformas digitales para conductas similares.

Concepto y características

En su sentido tradicional, "viejo verde" describe a un hombre mayor con comportamientos lujuriosos y de acoso sexual hacia personas más jóvenes.
En un contexto digital, podría referirse a personas mayores que emplean tecnologías digitales para acosar, manipular o mantener relaciones con personas mucho más jóvenes.
Esta conducta puede manifestarse en redes sociales, aplicaciones de mensajería y plataformas de citas digitales.
Suele involucrar conductas de acoso, manipulación de información o abuso de confianza.
Es importante distinguir entre el interés legítimo y el comportamiento abusivo o inapropiado.

Instrumentos y tecnología digital

Plataformas de redes sociales y aplicaciones de mensajería.
Herramientas de comunicación digital que facilitan el contacto y la influencia.
Posible uso de perfiles falsos o engañosos para acercarse a víctimas.
Técnica de manipulación emocional y social para obtener favores o control.

AZ
2025

40. Viejoverdes digitales

Normatividad peruana e internacional

Aunque el término específico "viejoverdes digitales" no está tipificado, las conductas de acoso digital, manipulación y abuso sexual están reguladas por la Ley N° 30096 de delitos informáticos y el Código Penal peruano.

La legislación prohíbe el acoso, la suplantación de identidad y los delitos sexuales cometidos mediante tecnología digital.

A nivel internacional, existen normativas y tratados que protegen a las personas contra el abuso y acoso en entornos digitales, promoviendo la seguridad y la dignidad.

Se fomenta la concienciación y prevención a través de políticas públicas y educación digital.

Sanciones

Penas privativas de libertad, multas y medidas de protección para las víctimas.

Aplicación de sanciones agravadas en casos de violencia o abuso sexual digital.

Medidas para bloquear y eliminar perfiles abusivos o fraudulentos.

Cooperación internacional para la persecución y condena de delitos digitales relacionados.

En conclusión, el concepto de "viejoverdes digitales" puede entenderse como el traslado a la esfera digital de comportamientos de personas mayores que usan tecnologías para conductas abusivas o de acoso hacia personas más jóvenes, con normativas y sanciones aplicables en Perú y en el ámbito internacional para proteger a las víctimas y garantizar el respeto en entornos digitales.

AZ
2025

40. Viejoverdes digitales . El CHILD GROOMING

- El child grooming es un conjunto de acciones realizadas por un adulto para establecer una relación de confianza con un menor, generalmente a través de medios tecnológicos, con el fin de manipularlo sexualmente.

- Este proceso incluye engañar al menor haciéndose pasar por una persona de edad similar, ganándose su amistad, creando vínculos emocionales y luego solicitando fotos, videos o encuentros de connotación sexual. El agresor, también llamado groomer, puede chantajear al menor con el material obtenido para seguir manipulándolo.

- El grooming es un delito que implica acoso y abuso sexual y puede causar daños psicológicos y emocionales profundos en la víctima. Se diferencia del ciberacoso en que su finalidad es la explotación sexual del menor y no solo causar daño emocional.

AZ
2025

40. Viejoverdes digitales . El CHILD GROOMING

HERRAMIENTAS TECNOLOGICAS USADAS PARA COMETER CHILD GROOMING

Las herramientas tecnológicas más usadas para cometer child grooming incluyen principalmente plataformas digitales y aplicaciones que permiten la comunicación directa e inmediata con menores, tales como:

Redes sociales (Facebook, Instagram, TikTok): Los agresores crean perfiles falsos o reales para acercarse al menor, ganarse su confianza y establecer contacto continuo.

Aplicaciones de mensajería instantánea (WhatsApp, Messenger, Telegram): Facilitan chats y videollamadas privadas donde se puede manipular al niño y solicitar imágenes o videos comprometidos.

Plataformas de juegos en línea: Los agresores entran en comunidades de videojuegos para interactuar con niños y adolescentes en espacios donde se sienten seguros y confiados.

Herramientas de videocaptura y edición de imágenes: Se utilizan para crear o manipular contenido sexual explícito, incluso usando tecnologías de inteligencia artificial (IA) para falsificar imágenes o videos comprometedores.

AZ
2025

40. Viejoverdes digitales . El CHILD GROOMING

HERRAMIENTAS TECNOLOGICAS USADAS PARA COMETER CHILD GROOMING

Software de control parental y vigilancia negativa: A veces los agresores explotan vulnerabilidades tecnológicas para evitar ser detectados, por ejemplo, usando perfiles alternativos o enmascarando su identidad digital.

Plataformas de intercambio de archivos y almacenamiento en la nube: Donde se comparte o guarda contenido ilegal de forma secreta.

Estos medios tecnológicos permiten que el agresor manipule la comunicación, amenace con la difusión de contenido privado (sextorsión) y mantenga el control sobre la víctima. La prevención incluye educación en seguridad digital, supervisión activa de menores, uso adecuado de controles parentales y políticas robustas en plataformas para detectar y bloquear conductas sospechosas.

En resumen, las herramientas tecnológicas usadas para el child grooming son aquellas que facilitan el contacto, la manipulación y la coerción sexual de menores a través de internet, y suelen incluir redes sociales, aplicaciones de mensajería, videojuegos, técnicas de manipulación visual y almacenamiento digital de material comprometedor.

AZ
2025

40. Viejoverdes digitales . El CHILD GROOMING

HERRAMIENTAS CONFIABLES PARA DETECTAR CUENTAS FALSAS Y CÓMO USARLAS

41. Vihing

AZ
2025

41. Vihing

El vishing, abreviatura de “voice phishing” o phishing por voz, es una técnica de ciberfraude en la que los atacantes utilizan llamadas telefónicas o mensajes de voz para engañar a las víctimas y obtener información confidencial, credenciales o cometer fraudes.

Concepto y características

Consiste en contactar a la víctima mediante llamadas telefónicas, mensajes pregrabados o voces manipuladas.

Los atacantes se hacen pasar por instituciones legítimas como bancos, organismos gubernamentales o empresas confiables para ganarse la confianza de la persona.

Utilizan software de modificación de voz para disfrazar su identidad, género o acento y hacer el engaño más creíble.

Pueden dejar mensajes urgentes que inducen a la víctima a devolver la llamada y revelar información sensible o realizar acciones que comprometen su seguridad.

A menudo se combinan con otras técnicas como el phishing y el smishing para aumentar la efectividad del ataque.

Instrumentos y tecnología digital

Software para modificación y simulación de voces (deepfake de voz).

Sistemas automatizados de llamadas masivas y mensajes pregrabados.

Herramientas para suplantación de números telefónicos (spoofing).

Uso de redes VoIP para ocultar ubicación e identidad.

Plataformas para coordinar ataques y compartir información obtenida.

AZ
2025

41. Vihing

Normatividad peruana e internacional

En Perú, el vishing está contemplado dentro de la Ley N° 30096 y el Código Penal como delito de fraude, suplantación de identidad y acceso ilegal a sistemas informáticos.
La legislación busca proteger la privacidad y seguridad de las comunicaciones.
A nivel internacional, el Convenio de Budapest y otras normativas regulan estas formas de ciberdelincuencia.
Se promueve la regulación tecnológica y campañas de educación para prevenir estos ataques.

Sanciones

Penas privativas de libertad, multas y decomiso de bienes para quienes realicen vishing.
Agravantes si afectan sectores estratégicos o causan perjuicios económicos importantes.
Medidas técnicas para bloquear llamadas fraudulentas y proteger a usuarios.
La cooperación internacional es clave para la persecución de los responsables.
En conclusión, el vishing es un método fraudulento de phishing por voz que busca engañar a las víctimas mediante llamadas telefónicas, regulado y sancionado en Perú e internacionalmente para proteger la seguridad y privacidad de las comunicaciones.

42. Virus,

AZ
2025

42. Virus.-

Los virus informáticos son programas maliciosos diseñados para propagarse de un sistema a otro, alterando el funcionamiento normal de los dispositivos infectados y causando daños, pérdidas de datos o robo de información.

Concepto y características

Son software malintencionado que se ocultan y ejecutan sin el consentimiento del usuario.
Pueden replicarse y transmitirse a través de medios como correos electrónicos, dispositivos USB, redes y archivos.
Tienen capacidad para modificar o destruir datos, interferir en el sistema operativo y facilitar la entrada de otros malware.
Algunos virus cuentan con técnicas para evitar detección, como cifrado o camuflaje en archivos legítimos.
Se clasifican en virus residentes, de arranque, de archivo, de macro, entre otros, dependiendo de su método de infección y propagación.

Instrumentos y tecnología digital

Archivos ejecutables infectados que contienen el código viral.
Vectores de infección: correos con adjuntos, descargas en internet, dispositivos externos.
Tácticas para adaptar el código que facilita eludir antivirus y permanecer activo en el sistema.
Interacción con otros malware para potenciar daños o controlar sistemas remotamente.

AZ
2025

42. Virus.-

Normatividad peruana e internacional

En Perú, los virus informáticos están regulados por la Ley N° 30096 y el Código Penal, que sancionan la creación, distribución y uso de software malicioso para dañar sistemas y robar información.

La normativa protege la integridad, disponibilidad y confidencialidad de los sistemas informáticos.

A nivel internacional, el Convenio de Budapest y otras regulaciones internacionales establecen mecanismos para combatir los delitos informáticos relacionados con virus.

Se promueve la educación, prevención y cooperación judicial para enfrentar estas amenazas.

Sanciones

Incluyen penas privativas de libertad, multas y decomiso para quienes elaboren o distribuyan virus.

Agravantes si afectan infraestructuras críticas como servicios públicos o sectores estratégicos.

Medidas técnicas para detección, eliminación y recuperación ante infecciones.

Cooperación internacional para la investigación y sanción de delincuentes cibernéticos.

En resumen, los virus informáticos son programas maliciosos que atacan y se propagan en sistemas digitales con intención dañina, regulados estrictamente en Perú e internacionalmente para proteger la seguridad digital con sanciones penales y técnicas específicas.

43. Whaling

AZ
2025

43. Whaling

El whaling es un tipo específico y avanzado de ataque de phishing dirigido exclusivamente a altos ejecutivos o personas con poder de decisión dentro de una organización, con el objetivo de obtener información confidencial o realizar transacciones fraudulentas.

Concepto y características

Es un ataque dirigido a “peces gordos” de las empresas, como CEOs, CFOs, directores o funcionarios clave.
Los correos electrónicos o mensajes falsificados aparentan venir de fuentes confiables, como otros altos ejecutivos o entidades legítimas.
Utilizan tácticas de ingeniería social muy sofisticadas, con mensajes personalizados, logos, firmas oficiales y un sentido de urgencia.
Suelen solicitar transferencias bancarias, revelar datos sensibles o realizar acciones que comprometen la seguridad corporativa.
Son difíciles de detectar debido a su alta personalización y apariencia legítima.

Instrumentos y tecnología digital

Correos electrónicos phishing personalizados que simulan autoridades internas.
Técnicas de suplantación de identidad y falsificación de correo electrónico.
Uso de ingeniería social, análisis previo para crear mensajes verosímiles.
Plataformas digitales para envío y recepción de mensajes.
Herramientas para ocultar o falsificar la identidad real del atacante.

AZ
2025

43. Whaling

Normatividad peruana e internacional

En Perú, está considerado dentro de delitos informáticos en la Ley N° 30096 y el Código Penal, que sancionan el acceso ilegal, el fraude y la suplantación de identidad.

A nivel internacional, el Convenio de Budapest y otras regulaciones promueven cooperación para prevenir y perseguir ataques dirigidos como el whaling.

La legislación protege la confidencialidad, integridad y disponibilidad de la información y promueve la ciberseguridad empresarial.

Se destaca la necesidad de capacitación y estrategias internas para prevenir estos ataques.

Sanciones

Penas de prisión, multas y decomiso de bienes para quienes realicen ataques de whaling.

Sanciones agravadas si afectan sectores estratégicos o generan daños económicos significativos.

Medidas técnicas para detectar, bloquear y neutralizar ataques, así como para restaurar la seguridad.

Cooperación internacional para investigación y procesamiento de responsables.

En conclusión, el whaling es un ataque sofisticado dirigido a altos ejecutivos para obtener información o realizar fraudes, regulado y sancionado en Perú e internacionalmente para proteger la seguridad de la información y los recursos de las organizaciones.

44. Whishing

AZ
2025

44. Whishing

El término "Whishing" es una variante especializada de phishing que busca atacar a individuos o pequeños grupos con algún criterio específico, como altos funcionarios o administradores de redes. Este término no es tan común como otros derivados de phishing, pero se emplea para describir ataques dirigidos que utilizan técnicas de ingeniería social combinadas con software malicioso para robar información.

Concepto y características

Whishing se enfoca en ataques muy dirigidos, diseñados especialmente para personas o grupos con alto valor para el atacante.
El malware puede estar "dormido" esperando el momento oportuno para activarse y robar información.
Utiliza ingeniería social para ofrecer mensajes o enlaces que parecen legítimos y confiables.
Puede combinarse con virus, spyware, keyloggers, troyanos para maximizar el daño y el robo de datos.
Es utilizado en contextos donde la información específica o el acceso a sistemas clave es crítico.

Instrumentos y tecnología digital

Uso de malware avanzado que se camufla y permanece inactivo hasta ser activado.
Ataques dirigidos que combinan técnicas de phishing avanzado con propagación de software malicioso.
Plataformas digitales para envío de mensajes específicos y análisis de comportamientos para detectar y atacar objetivo.

AZ
2025

44. Whishing

Normatividad peruana e internacional

Aunque el término específico "whishing" puede no estar descrito en leyes, sus conductas asociadas se regulan en la Ley N° 30096 y el Código Penal peruano.

Se sancionan delitos como acceso ilegal, fraude informático, suplantación de identidad y distribución de malware.

A nivel internacional, el Convenio de Budapest y otros tratados establecen marcos para perseguir delitos informáticos graves y especializados.

La normativa busca proteger la integridad, confidencialidad y disponibilidad de la información crítica y personal.

Sanciones

Penas de prisión, multas y decomiso para quienes ejecuten o faciliten este tipo de ataques especializados.

Mayor severidad si afectan infraestructuras críticas, datos sensibles o actividades estatales.

Medidas técnicas y jurídicas para detección, bloqueo y mitigación, así como restauración de sistemas afectados.

Cooperación internacional para la persecución y condena de responsables.

En resumen, el whishing es un tipo avanzado y dirigido de ataque informático basado en phishing combinado con malware, regulado y sancionado en Perú y a nivel internacional para proteger la seguridad digital y la información crítica.

45. Whistleblowers

AZ
2025

45. Whistleblowers

Los whistleblowers o denunciantes son personas que revelan información sobre actividades ilícitas, corrupción, fraudes u otras conductas ilegales dentro de organizaciones, ya sean públicas o privadas, con el fin de proteger el interés general y promover la transparencia.

Concepto y características

Son individuos que informan de buena fe sobre irregularidades graves.
Suelen hacerlo a través de canales internos de denuncia o públicos, manteniendo en ocasiones anonimato o confidencialidad.
Pueden ser empleados, funcionarios, o cualquier persona con acceso a información relevante.
Su acción busca prevenir daños, proteger derechos y garantía el cumplimiento legal.
Requieren protección para evitar represalias y amenazas.

Instrumentos y tecnología digital

Canales internos de denuncias electrónicos o físicos.
Plataformas digitales seguras para garantizar confidencialidad y anonimato.
Herramientas de seguimiento y gestión de denuncias.
Sistemas de encriptación y protección de datos para resguardar información.
Mecanismos de verificación y auditoría interna para investigar las denuncias.

AZ
2025

45. Whistleblowers

Normatividad peruana e internacional

En Perú, la Ley N° 30424 regula la responsabilidad administrativa de personas jurídicas e incluye mecanismos de protección para whistleblowers.

El Decreto Legislativo 1327 establece disposiciones adicionales para proteger a los denunciantes.

A nivel internacional, la Convención de Naciones Unidas contra la Corrupción, la Convención Interamericana contra la Corrupción y la Directiva 2019/1937 de la Unión Europea establecen estándares para la protección y mecanismos de denuncia.

Las normas requieren la implementación de sistemas seguros, confidenciales y efectivos para las denuncias, garantizando protección contra represalias.

Sanciones

Se sanciona cualquier tipo de represalia, intimidación o discriminación contra los denunciantes.

Penas y multas para quienes incumplan la protección de los whistleblowers o manipulen información.

Medidas judiciales y administrativas para asegurar la investigación adecuada de denuncias.

Protección integral para garantizar la seguridad física y legal del denunciantes.

En conclusión, los whistleblowers son actores fundamentales en la lucha contra la corrupción y la ilegalidad, protegidos por normativas específicas en Perú e internacionalmente para asegurar su integridad y promover la transparencia en organizaciones públicas y privadas.

AZ
2025

...

UNIDAD II:

Legislación y Marco Normativo

- La Ley N° 30096, Ley de Delitos Informáticos
- Convenio de Budapest sobre Ciberdelincuencia.
- Leyes de protección de datos personales.
- Responsabilidad penal de personas naturales y jurídicas.

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos:

Esta ley tiene por objeto prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos y otros bienes jurídicos mediante el uso de tecnologías de la información. Algunos aspectos relevantes:

- Prevención y sanción de delitos como acceso ilícito a sistemas, daño o alteración de datos, ataques a la integridad de sistemas, suplantación de identidad, difusión de pornografía infantil y fraudes electrónicos.
- Incorporación en 2025 de agravantes y penas mayores para delitos cometidos con el uso indebido de inteligencia artificial o tecnologías similares.
- Penalización del abuso de mecanismos y dispositivos informáticos utilizados para cometer delitos informáticos.
- Modificaciones en el Código Penal para ampliar tipos penales y sanciones ligados a delitos informáticos.
- La aplicación de esta legislación busca responder a la evolución tecnológica y el creciente uso de herramientas digitales que requieren protección específica en el ámbito legal.

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CONTENIDO DE LA LEY 30096**

La Ley N° 30096, Ley de Delitos Informáticos en Perú, actualizado a 2025, está estructurado en siete capítulos principales que se resumen a continuación:

- Capítulo I: Finalidad y objeto de la ley.
- Capítulo II: Delitos contra datos y sistemas informáticos (artículos relacionados con acceso ilícito, atentado a la integridad de datos y sistemas).
- Capítulo III: Delitos informáticos contra la indemnidad y libertad sexuales (como proposiciones sexuales a menores por medios tecnológicos).
- Capítulo IV: Delitos informáticos contra la intimidad y el secreto de las comunicaciones.
- Capítulo V: Delitos informáticos contra el patrimonio.
- Capítulo VI: Delitos informáticos contra la fe pública.
- Capítulo VII: Disposiciones comunes (sobre aspectos procedimentales y coordinación).

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CAPÍTULO I: FINALIDAD Y OBJETO DE LA LEY**

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

- **Artículo 1. Objeto de la Ley**
  - **P**revenir y sancionar las conductas ilícitas que
    - afectan los sistemas
    - Afectan a los datos informáticos
    - afectan otros bienes jurídicos de relevancia penal,
      - mediante la utilización de tecnologías de la información o de la comunicación,
      - con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia
        - con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **Capítulo II: Delitos contra datos y sistemas informáticos (artículos relacionados con acceso ilícito, atentado a la integridad de datos y sistemas). LEY 30096 PERU**
- El Capítulo II de la Ley N° 30096, que trata sobre los delitos contra datos y sistemas informáticos, presenta un marco normativo riguroso que protege bienes jurídicos esenciales como la confidencialidad, integridad y disponibilidad de los datos y sistemas tecnológicos. Desde una perspectiva jurídica, esta parte de la ley tipifica conductas delictivas fundamentales que afectan la seguridad cibernética, como el acceso ilícito a sistemas vulnerando medidas de protección y el atentado contra la integridad tanto de datos como de los sistemas informáticos.
- El acceso ilícito se sanciona severamente, estableciendo penas proporcionales que buscan disuadir la vulneración de sistemas mediante intrusiones no autorizadas. La integridad de los datos, columna vertebral de la confianza tecnológica, recibe especial tutela, castigando actividades que dañen, alteren o hagan inaccesible la información, lo que puede generar daños económicos y sociales graves. Asimismo, la protección del funcionamiento adecuado de los sistemas informáticos garantiza el soporte tecnológico indispensable para diversas actividades públicas y privadas.
- Cabe destacar que la legislación contempla agravantes significativos, como la comisión de estos delitos en calidad de miembros de organizaciones criminales, el abuso de posiciones privilegiadas con acceso a información sensible, y el uso de tecnologías avanzadas como la inteligencia artificial para perpetrar estas conductas. Igualmente, la ley prevé exenciones cuando las acciones son realizadas en el marco de pruebas autorizadas para la defensa de los siste

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CAPÍTULO III: DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES (COMO PROPOSICIONES SEXUALES A MENORES POR MEDIOS TECNOLÓGICOS).**
- El Capítulo III de la Ley N° 30096, que aborda los delitos informáticos contra la indemnidad y libertad sexuales, representa un avance crucial en el marco jurídico peruano para proteger especialmente a los niños, niñas y adolescentes frente a las nuevas formas de violencia sexual facilitadas por tecnologías de la información.
- Desde un enfoque crítico, este capítulo tipifica como delito grave las proposiciones sexuales a menores por medios tecnológicos, tales como internet, con el objetivo de obtener material pornográfico o inducir a actos de connotación sexual. La sanción penal, que puede ser de seis a nueve años de prisión, refleja la gravedad y el rechazo absoluto a estas conductas que vulneran derechos fundamentales y la integridad moral de las víctimas.
- Este cuerpo normativo también reconoce la relevancia de las pruebas digitales como elementos decisivos para la investigación y persecución penal, otorgando validez jurídica a evidencias obtenidas mediante tecnologías siempre que se respeten los principios de legalidad, autenticidad e integridad. Sin embargo, la efectividad de estas disposiciones depende en gran medida de la capacidad del sistema penal y de la sensibilización social para enfrentar el problema de la violencia sexual digital, aún caracterizado por altas tasas de impunidad y revictimización.

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- Capítulo IV: Delitos informáticos contra la intimidad y el secreto de las comunicaciones
- El Capítulo IV de la Ley N° 30096 de Perú, que regula los delitos informáticos contra la intimidad y el secreto de las comunicaciones, es una pieza fundamental del marco jurídico para proteger derechos esenciales en la era digital.
- Desde un punto de vista jurídico, este capítulo sanciona conductas que vulneran la esfera privada de las personas, como la interceptación, grabación, difusión o divulgación no autorizada de comunicaciones privadas, incluyendo las emisiones electromagnéticas y electrónicas que puedan contener información reservada. La ley establece penas proporcionales para quienes, de manera deliberada e ilegítima, atenten contra el secreto y la confidencialidad de las comunicaciones, asegurando la protección de la intimidad frente a la invasión tecnológica.
- La norma enfatiza la protección del derecho a la privacidad como un bien jurídico protegido, reconociendo que en la actualidad la información circula masivamente en soportes digitales y redes, por lo que una adecuada tutela penal es indispensable para salvaguardar la confianza y seguridad de los usuarios. Además, esta regulación contribuye a prevenir delitos conexos, como el chantaje, la difamación o el acoso que pueden derivar de la violación de secretos.

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CAPÍTULO V: DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO.**
- El Capítulo V de la Ley N° 30096, que regula los delitos informáticos contra el patrimonio, constituye una respuesta jurídica integral frente a las nuevas formas de afectación patrimonial generadas por el uso de tecnologías de la información y comunicación. Desde una perspectiva jurídica, este capítulo destaca la protección del patrimonio como un bien jurídico vulnerable a través de conductas ilícitas como el fraude informático.
- El artículo clave es el que tipifica el fraude informático, definido como la obtención de un provecho ilícito para sí o para otro, mediante la manipulación tecnológica como el diseño, alteración, borrado o clonación de datos o programas informáticos, afectando la propiedad de terceros. Este delito se sanciona con pena privativa de libertad y multas, reflejando la gravedad de dañar la confianza y seguridad que sustentan las transacciones y actividades económicas en el entorno digital.
- Es importante resaltar la caracterización del sistema informático como bien mueble de naturaleza patrimonial, cuya afectación directa implica la alteración o detrimento de un patrimonio tanto de personas naturales como jurídicas. La ley cumple así la función de aggiornamiento normativo para enfrentar la ciberdelincuencia económica, adaptando conceptos clásicos del derecho penal a la realidad tecnológica.

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CAPÍTULO VI: DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA.**
- El Capítulo VI de la Ley N° 30096 constituye un avance significativo en la legislación peruana al abordar los delitos informáticos contra la fe pública, particularmente la suplantación de identidad. Desde un enfoque legal, este capítulo protege un bien jurídico fundamental que es la confianza pública en la identidad de las personas y entidades en el ámbito digital, esencial para la seguridad y legalidad de las transacciones y relaciones sociales.
- La norma tipifica la suplantación de identidad que se realiza mediante tecnologías digitales, estableciendo penas privativas de libertad proporcionales, con agravantes cuando la víctima es menor de edad o se ocasionan perjuicios materiales o morales significativos. Esta tipificación responde a la necesidad de enfrentar nuevos desafíos derivados del uso masivo de medios digitales, donde la falsificación de identidad puede facilitar delitos como fraudes, extorsiones y otras formas de engaño electrónico.
- Además, el capítulo contempla sanciones para quienes fabrican, venden o distribuyen herramientas informáticas destinadas a facilitar estos delitos, manifestando una mirada integral que busca cortar la cadena delictiva desde la provisión de medios hasta la ejecución material del delito..

AZ
2025

La Ley N° 30096 – Ley de Delitos Informáticos / Contenido:

- **CAPÍTULO VII: DISPOSICIONES COMUNES (SOBRE ASPECTOS PROCEDIMENTALES Y COORDINACIÓN).**
- El Capítulo VII de la Ley N° 30096, que contiene las disposiciones comunes, es un componente esencial para garantizar la eficacia y coherencia en la aplicación de la ley contra los delitos informáticos en el Perú. Jurídicamente, este capítulo establece aspectos procedimentales y organizacionales que permiten una acción penal ágil y coordinada en un contexto tecnológico dinámico y complejo.
- Se destaca la regulación sobre el abuso de mecanismos y dispositivos informáticos, penalizando la fabricación, diseño, desarrollo, venta, facilitación o provisión de herramientas que puedan ser utilizadas para cometer delitos informáticos. Esta previsión es clave para atacar la cadena de producción y distribución de medios técnicos ilícitos que potencian los ciberdelitos.
- Además, el capítulo regula la cooperación interinstitucional, estableciendo protocolos de coordinación entre la Policía Nacional, el Ministerio Público y otros organismos competentes para el manejo de evidencia digital, investigaciones, intervenciones y seguimiento de casos. También habilita a los fiscales para autorizar la actuación de agentes encubiertos en investigaciones complejas de ciberdelitos, a fin de preservar la eficacia y legalidad del proceso.
- Finalmente, se establece un marco adecuado para el control judicial en la autorización y supervisión de las medidas extremas, asegurando el respeto a los derechos fundamentales y garantías procesales en la persecución penal de delitos informáticos.

UNIDAD II:

EL CONVENIO DE BUDAPEST sobre la CIBERDELINCUENCIA

- Convenio de Budapest sobre Ciberdelincuencia.

AZ
2025

EL CONVENIO DE BUDAPEST sobre la CIBERDELINCUENCIA:

- El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 bajo el amparo del Consejo de Europa y en vigor desde 2004, es el primer tratado internacional para combatir los delitos informáticos
- El Convenio tipifica delitos informáticos como:
  - acceso ilícito,
  - interceptación ilegítima,
  - fraudes,
  - delitos relacionados con contenido de pornografía infantil y
  - violaciones a la propiedad intelectual
- Establece procedimientos comunes para la investigación y persecución penal, incluyendo la obtención de evidencia electrónica, vigilancia de comunicaciones y cooperación judicial transnacional.
- Facilita la colaboración rápida y eficiente entre estados para responder a crímenes cibernéticos, promoviendo la seguridad digital y el respeto a los derechos humanos, como la privacidad y la libertad de expresión, en el contexto del ciberespacio.

AZ
2025

EL CONVENIO DE BUDAPEST sobre la CIBERDELINCUENCIA:

- El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 bajo el amparo del Consejo de Europa y en vigor desde 2004, es el primer tratado internacional para combatir los delitos informáticos
- El Convenio tipifica delitos informáticos como:
  - acceso ilícito,
  - interceptación ilegítima,
  - fraudes,
  - delitos relacionados con contenido de pornografía infantil y
  - violaciones a la propiedad intelectual
- Establece procedimientos comunes para la investigación y persecución penal, incluyendo la obtención de evidencia electrónica, vigilancia de comunicaciones y cooperación judicial transnacional.
- Facilita la colaboración rápida y eficiente entre estados para responder a crímenes cibernéticos, promoviendo la seguridad digital y el respeto a los derechos humanos, como la privacidad y la libertad de expresión, en el contexto del ciberespacio.

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

UNIDAD II:

DELITOS INFORMÁTICOS CONCLUSIONES

- Felipe Villavicencio

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

1) La finalidad de la *Ley de Delitos Informáticos* es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fe pública y la libertad sexual cometidos mediante la utilización de las TI C.

2) La figura penal **de *acceso ilícito***, regulada en el artículo 2, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de vulnerar las medidas de seguridad de un sistema informático.

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

3) - La figura penal de ***atentado contra la integridad de datos informáticos***, regulada en el artículo 3, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos.

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

4) - La figura penal **de *atentado contra la integridad de sistemas informáticos***, regulada en el artículo 4, se clasifica como un *delito de resultado*, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo, sino que es necesario un resultado posterior que consiste en impedir el acceso, imposibilitar el funcionamiento del sistema informático o impedir la prestación de su servicio

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

5) - La figura penal de ***proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos,*** regulada en el artículo 5, es un *tipo de tendencia interna trascendente* porque presenta un elemento subjetivo distinto del dolo que denota una especial intención del agente, por tanto esta figura se clasifica como un ***delito de resultado cortado***, porque el agente persigue un resultado posterior el cual es obtener material pornográfico o alguna actividad sexual.

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

6) La figura penal de ***tráfico ilegal de datos***, regulada en el artículo 6, queda derogada por la única disposición complementaria derogatoria de la Ley 30171. Este articulo derogado fue incorporado al Código Penal (Artículo 154-A; *tráfico ilegal de datos personales*)

7) - La figura penal de ***interceptación de datos informáticos***, regulada en el artículo 7, es un ***delito de peligro abstracto***, y se clasifica como un ***delito de mera actividad*** porque en este ilícito el delito queda consumado en el mismo acto de interceptar datos informáticos

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

8) - La figura penal de ***fraude informático***, regulada en el artículo 8, se clasifica como un ***delito de resultado***, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo legal (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático), sino que es necesario un resultado posterior que consiste en causar un perjuicio a tercero.

9) - La figura penal de ***suplantación de identidad***, regulada en el artículo 9, se clasifica como un *delito de resultado*, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo (suplantar la identidad de una persona natural o jurídica), sino que es necesario un

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

10) La figura penal de ***abuso de mecanismos y dispositivos informáticos***, regulada en el artículo 10, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de fabricar, diseñar, vender, etcétera; el mecanismo o los programas orientados a cometer diversos delitos previstos en esta ley.

11) - La *Décima disposición complementaria final* regula la **sanción administrativa para las personas jurídicas** que están bajo la supervisión de la SBS que incumplan una orden judicial consistente en brindar información sobre el secreto bancario.

AZ
2025

LOS DELITOS INFORMATICOS

- CONCLUSIONES.-

-

- La *Undécima disposición complementaria final* regula la sanción administrativa para las personas jurídicas que están bajo la supervisión de OSI PTE L que incumplan una orden judicial consistente en brindar información sobre la intervención, grabación o registro de las comunicaciones telefónicas.

5. Glosario

MUCHAS GRACIAS ...