

“Delitos contra la intimidad, allanamiento y otros delitos informáticos. Responsabilidad penal de las personas jurídicas en delitos relacionados con la corrupción”

Julio César Tapia Cárdenas

Mayo 2023



CONTENIDO

01

Delitos contra la intimidad

02

Delitos informáticos

03

Corrupción y responsabilidad penal de la persona jurídica



PGE

Procuraduría General del Estado



1

Delitos contra la intimidad

Intrusión al ámbito privado de desarrollo





PGE

Procuraduría General
del Estado

Centro de
Formación y
Capacitación



Gobierno del Peru



BICENTENARIO
DEL PERÚ
2021 - 2024

VIOLACION DE LA INTIMIDAD

Violación de la intimidad

Artículo 154. - El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años.

La pena será no menor de uno ni mayor de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista.

Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

“Artículo 154-A. Tráfico ilegal de datos personales

El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior.” (*)

(*) Artículo incorporado por el Artículo 5 de la Ley N° 30171, publicada el 10 marzo 2014.



PGE

Procuraduría General
del Estado

Centro de
Formación y
Capacitación



Gobierno del Peru



BICENTENARIO
DEL PERÚ
2021 - 2024

“Artículo 154-B. - Difusión de imágenes, materiales audiovisuales o audios con contenido sexual

El que, sin autorización, difunde, revela, publica, cede o comercializa imágenes, materiales audiovisuales o audios con contenido sexual de cualquier persona, que obtuvo con su anuencia, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años y con treinta a ciento veinte días-multa.

La pena privativa de libertad será no menor de tres ni mayor de seis años y de ciento ochenta a trescientos sesenta y cinco días-multa, cuando concorra cualquiera de las siguientes circunstancias:

1. Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges.
2. Cuando para materializar el hecho utilice redes sociales o cualquier otro medio que genere una difusión masiva.” (*)

(*) Artículo incorporado por el Artículo 2 del Decreto Legislativo N° 1410, publicado el 12 septiembre 2018.

"Artículo 155. - Agravante por razón de la función

Si el agente es funcionario o servidor público y, en ejercicio del cargo, comete el hecho previsto en los artículos 154 y 154-A, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36 incisos 1, 2 y 4.

Si el agente es funcionario o servidor público y, en ejercicio del cargo, comete el hecho previsto en los artículos 154 y 154-A y la información tenga su origen a partir de la aplicación de la medida de la localización o geolocalización, la pena será no menor de seis ni mayor de ocho años e inhabilitación conforme al artículo 36 incisos 1, 2 y 4."

Uso indebido de archivos computarizados

Artículo 157. - El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

"Artículo 158. - Ejercicio de la acción penal

Los delitos previstos en este Capítulo son perseguibles por acción privada, salvo en el caso del delito previsto en los artículos 154-A y 155."

2

DELITOS INFORMÁTICOS

**NUEVAS FORMAS DE DELINCUENCIA
PERFIL DEL DELINCUENTE INFORMÁTICO
EVIDENCIA DIGITAL**



PGE

Procuraduría General
del Estado

Centro de
Formación y
Capacitación



Gobierno del Peru



BICENTENARIO
DEL PERÚ
2021 - 2024

DELITOS EN Y DESDE LA RED

Internet es una herramienta esencial en nuestra vida. Gracias a esta, compartimos información, trabajamos y nos comunicamos con familiares y amigos. Pero también ha traído problemas, pues es usada para realizar actos ilícitos. Los delitos informáticos, que afectan a muchas personas en el mundo, aumentan día a día.
¿Qué podemos hacer?



PGE

Procuraduría General
del Estado

Centro de
Formación y
Capacitación



Gobierno del Peru



BICENTENARIO
DEL PERÚ
2021 - 2024

Los delitos más comunes en el Perú son los cometidos contra el patrimonio –aquellos que por medio de ataques atentan contra cuentas bancarias– y la suplantación de identidad.



Ataque replay

Consiste en una repetición de transmisión de datos con el objetivo de realizar un "ataque enmascarado" para recabar información de la computadora atacada.

Ataque de día cero

Este tipo de ataque explota los puntos débiles o agujeros de seguridad de algún programa. Los sistemas operativos y softwares de uso masivo son los principales puntos de ataque.

Correos electrónicos

¿Quién no ha encontrado en su bandeja de entrada correos de empresas o personas desconocidas que hacen referencia a campañas o las famosas "cadenas"? Dicho mensajes no siempre son obra de delincuentes informáticos, pero se corre el riesgo de que al abrirlos o linkear, nos encontremos ante los correos spam o correos basura, que no tienen información de utilidad. Basta con dar un clic en las páginas que hacen mención para que nos redireccionen a sitios desconocidos en los cuales nos solicitan datos personales.

Spam

Conocemos como spam o correo basura a los correos electrónicos de carácter comercial que recibimos sin que los

hayamos solicitado. Estos correos son enviados de forma masiva a millones de personas y brindan, por lo general, información sobre productos o servicios.

Cadenas o hoaxes

Son mensajes masivos sobre noticias o falsas alarmas de cualquier tipo, en los que se nos pide que enviemos el mensaje a nuestros conocidos. Estos mensajes son usados para obtener las cuentas de correo electrónico de más personas. Al reenviarlos, mandamos a gente que conocemos todas las cuentas de correo electrónico que ya han sido reenviadas mensaje tras mensaje en esta cadena. No todas las cadenas sirven para este fin. Algunas sirven realmente para buenas causas y no tienen nada de malicioso.

Pop-ups

Son el medio que utilizan los hackers para saturar a un usuario o computadora. El ataque consiste en mandar un archivo malicioso enmascarado en un mail o un archivo ejecutable, el cual, al activarlo, permite la aparición de innumerables ventanas emergentes (de ahí el nombre "pop-up"), que el usuario trata de cerrar una por una, mientras que el atacante se infiltra en el sistema y extrae información o logra el propósito de su ataque.



Ley de Delitos Informáticos - Ley Número 30096

Posted on: 6 March 2023 By: ReYDeS

La Ley 30096 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.

La Ley Número 30171 modifica los siguientes artículos: art. 2do (Acceso ilícito), art. 3ero (Atentado a la integridad de datos informáticos), art. 4to (Atentado a la integridad de sistemas informáticos), art. 5to (Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos), art. 7mo (Interceptación de datos informáticos), art. 8vo (Fraude informático) y art. 10mo (Abuso de mecanismos y dispositivos informáticos) de la Ley 30096

Una actividad ilícita en auge es la venta de información de las llamadas "bases de datos" de entidades como bancos y universidades.

tas Patrias, vulneró la seguridad de varias páginas web del Gobierno. Entre ellas, la página de la Presidencia de la República (www.presidencia.gob.pe) y los sitios web de algunas municipalidades. Este ataque se dio como parte de las actividades de su "Operación Independencia". Una acción similar fue efectuada en México, el 15 de setiembre del 2011, mediante esta, Anonymous inhabilitó desde la mañana las páginas de las principales entidades gubernamentales de dicho país.

Correo fraudulento

En noviembre del 2013, luego de las elecciones de los nuevos regidores de Lima, circuló por Internet un correo falso de la Oficina Nacional de Procesos Electorales (ONPE), en el que se "obligaba a abrir" un archivo por tener "multas graves".

Ante ello, la ONPE señaló que esos correos electrónicos eran fraudulentos, debido a que no existía ninguna disposición al respecto. Después de que la ONPE se manifestara sobre el tema, se iniciaron las investigaciones

para identificar a las personas que enviaron los correos falsos.

Venta de información

Una actividad ilícita que ha cobrado auge en nuestro país es la venta de información contenida en las llamadas "bases de datos" de entidades bancarias, universidades, administradoras de fondos de pensiones, entidades del Gobierno, etcétera.

Esta información, que en teoría debe ser de estricto uso de las organizaciones que las poseen, es obtenida por organizaciones delictivas para recabar datos de potenciales víctimas de estafas, extorsiones e incluso secuestros.

Las investigaciones policiales señalan que los precios de las bases de datos ofrecidas en las diversas galerías de

500

BOBOS DIARIOS
POR INTERNET
SE PRODUCIAN
EN EL PERÚ EN
EL 2013.

venta de computadoras y accesorios en la avenida Garcilaso de la Vega oscilan entre los S/ 400 y los S/ 800. Quienes ofrecen esta información cometen el delito contra el patrimonio en la modalidad de receptación y delito informático.





¿QUE PODEMOS HACER?

Además de la preparación que deben tener nuestros jueces, fiscales y fuerza policial, es importante que



EVIDENCIA DIGITAL

PRINCIPIOS DEL PERITAJE

- **OBJETIVIDAD**  Requisito del fiscal que dirige la investigación así como del perito informático que analiza la información.
- **LEGALIDAD**  Perito: preciso en conclusiones y metodología utilizada. Su actuación es acorde a la legislación de la actividad.
- **IDONEIDAD**  Las herramientas usadas son idóneas y validadas para apoyar las conclusiones.
- **INALTERABILIDAD**  Debido cumplimiento de la cadena de la custodia que asegure que no hay alteración del peritaje.

Definición, importancia y tratamiento de: **La Evidencia Digital**

Es un registro almacenado en un dispositivo informático, se transmite bajo una red y puede tener valor probatorio. Se considera evidencia a cualquier información sujeta a intervención humana (medio tecnológico),

Importancia: necesidad de demostrar fehacientemente al sospechoso en responsable.

- Correcto tratamiento de la evidencia digital - documentación y justificación
- para que sea admisible – la evidencia sea obtenida respetando las garantías y procedimientos legales, previa autorización judicial.

Fuentes de evidencia digital; Sistema de computación abiertos, sistemas de comunicación y sistemas convergentes de computación.

CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL

- VOLÁTIL → Si no es preservada adecuadamente puede cambiar o variar.
- DUPLICABLE → Puede ser duplicada de manera exacta y copiada como si fuese original.
- ALTERABLE Y MODIFICABLE → Con herramientas adecuadas es fácil de destruir, alterar y modificar.
- ELIMINABLE → Con herramientas adecuadas puede ser eliminada por completo



ASEGURAMIENTO DE LA ESCENA DEL DELITO

Quienes participen en diferentes actos de aseguramiento o análisis lo harán bajo:
Nuevo Código Procesal Penal –Decreto Legislativo n° 957.

Artículo 67: El aseguramiento por funcionarios de la Policía Judicial (conocimiento técnico avanzado) en cuanto a la evidencia digital.

Artículo 68: En la conducción fiscal se llevara a cabo varias tareas:

- a) Recoger y conservar objetos relacionados con el delito.
- b) Levantar planos, fotografías, grabaciones, etc.
- c) Efectuar bajo inventario secuestros e incautaciones necesarias.
 - > en casos de flagrancia o peligro inminente

Todo lo actuado quedará sentado en actas detalladas que se entregarán al Fiscal.

Los investigadores en una escena del crimen debe cumplir:

- Establecer los parámetros de la escena del delito
- Observación, valoración y planificación
- Delimitar la escena del delito
- Asegurar la identificación de testigos, policías médicos, bomberos, personal especializado.
- Establecer las medidas de seguridad
- Facilitar los primeros auxilios
- Asegurar físicamente la escena
- Asegurar físicamente las evidencias
- Documentar la escena



RECONOCIMIENTO E IDENTIFICACIÓN DE: LA EVIDENCIA DIGITAL

DONDE ENCONTRAR LA EVIDENCIA

1. Dispositivos de almacenamiento informático

- Unidades de disco rígido internas
- Discos rígidos externos
- Medios extraíbles
- Pendrive (USB)
- Tarjeta de memoria

Posibles evidencias:

mensajes de correo, historial de navegación, Chat de Internet, formatos de archivos (JPG, PNG, GIF, BMP, TIF)

2. Dispositivos portátiles

- Teléfonos celulares
- Smartwatches
- PDAs
- Dispositivos digitales multimedia
- Cámaras digitales
- Sistemas de posicionamiento global (GPS)
- Reproductores
- Video filmadoras
- Localizador
- Sistemas en vehículos
- Cámaras de seguridad

Posibles evidencias:

Listado de llamados, mensajes recibidos y enviados, páginas de Internet visitadas, datos de localización geográfica, aplicaciones de software) archivos de imágenes, base de datos y registros, mensajes de voz, redes Wi-Fi detectadas.

RECONOCIMIENTO E IDENTIFICACIÓN DE: LA EVIDENCIA DIGITAL

DONDE ENCONTRAR LA EVIDENCIA

3. Dispositivos periféricos

- Teclado • Mouse • Parlantes • Cámaras • Fax
- Teléfonos • Router • Módem • Impresoras • Escáners • Fotocopiadoras • Contestadores automáticos

Posibles evidencias:

Entrada y salida de números de teléfonos y fax, llamados recientes, fax en la memoria, documentos impresos, impresiones dactilares, ADN, etc. Estos dispositivos pueden aportar evidencia física que permita vincular al usuario con el dispositivo digital incautado.

4. Redes de computadoras: computadoras conectadas por cables de datos o conexiones inalámbricas que comparten recursos e incluso de impresoras, periféricos (hubs, switches y routers).

Posibles evidencias:

Pruebas de software, documentos, fotos, archivos de imágenes, mensaje de correo y archivos adjuntos, base de datos, historial de navegación de Internet, registros de eventos y chat, datos almacenados en dispositivos externos.

Adquisición y captura de: La Evidencia Digital

➤ EVIDENCIA AL RECOLECTAR:

De preferencia grandes volúmenes de información: computadoras, discos rígidos.

Si es muy voluminoso o afecte derecho de terceros es posible el (triage).

Si hay autorización judicial y se tiene software necesario, podrá decidirse con el experto informático la realización de una copia o imagen forenses sobre la escena.

La excepción es **la investigación en vivo**, se debe evitar acceder al contenido de los elementos electrónicos para evitar su contaminación.

Se debe tener en cuenta el orden de volatilidad: contenido de registro, tablas de ruteo, caché, procesos de ejecución, memoria RAM, almacenamiento masivo, almacenamiento remoto y de resguardo y respaldo. Adquisición de datos volátiles.

Adquisición y captura de: La Evidencia Digital

- **DIFERENTES ESCENARIOS:** Se presentan III escenarios para poder proceder diligentemente.
- **EMBALAJE Y ROTULADO:** Este será primer paso del procedimiento de cadena de custodia
- **ELEMENTOS Y MATERIALES PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL:** Equipos de fotografía y video, etiquetas, cartón, guantes, etc.
- **DOCUMENTACIÓN Y REGISTRO DE LO ACTUADO:** Previsto por los Artículos - 214 al 217 del NCPP solicitados por Fiscal al Juez competente.
 - Cfr. Artículos 67 y 68 del NCPP
 - Artículos 120, 155, 157, 158, 172/181, 177, 178, 202, 203, 208, 210, 214/217, 226, 227, 230 y 231 del Código Procesal Penal del Perú

DISPOSITIVOS TELEFÓNICOS

Ante el hallazgo de equipos móviles y/o cualquier otro dispositivo que utilice la red de comunicación se adoptara recaudos adicionales:

- No manipular el teléfono.
- Dejar constancia en el acta del lugar del hallazgo y usuario o poseedor
- Dejar constancia si estaba apagado o encendido.
- Los que no tengan batería extraíble – MODO AVIÓN – (IPhone)
- Si esta apagado, mantenerlo así.
- Detectar numero de IMEI – CHIP número.
- Preservar e celular y batería en BOLSA TRANSPARENTE.

- Elementos que nos permite información investigativa:
 - SIM – código de investigación de la línea telefónica.
 - IMEI - código de identificación de aparato
 - CELDA – Espacio de cobertura de telefonía celular

Extracción forense de celulares: Obtención de información

- Permite recuperar y analizar evidencias de teléfonos móviles
- Registros e historial de llamadas aún los borrados de la SIM
- Contactos
- Datos de teléfono (IMEI, número de teléfono)
- Mensajes de texto (SMS) aún los borrados de la SIM. Redes sociales (Facebook, WhatsApp, twitter, viber, etcétera)
- Fotografías
- Videos
- Archivos de sonido
- Información de localización de la SIM
- Clonación del ID de la SIM

OTROS APARATOS ELECTRONICOS:

- TELÉFONOS INALÁMBRICOS: Llamadas, números registrados, nombres, etc.
- APARATOS DE MENSAJERÍA INSTANTÁNEA, BEEPERS: Numéricos, Alfanuméricos, de Voz, de dos vías.
- MAQUINAS DE FAX: Listas de marcado rápido, fax guardados, líneas de encabezado, hora y fecha de transmisión de Fax. (evitar apagar el Fax al hallarla)
- IMPRESORAS: Datos de la red, número de serie, versión de firmware, documentos impresos, pruebas biológicas. (ADN)
- SMARTWATCHES: GPS, NFC, WIF, redes celulares, se utiliza para recuperar datos y controlar dispositivos.

OTROS APARATOS ELECTRONICOS:

- **DISPOSITIVOS DE ALMACENAMIENTO:** Dispositivos magnéticos, de estado solido, memorias solidas, dispositivos ópticas.

CORREOS ELECTRONICOS:

- Permite enviar y recibir cartas escritas ya sea desde la computadora, teléfono celular, Tablet y/o cualquier otro dispositivo con acceso a internet.
- En ocasiones es necesario seguir el rastro de los Correos Electrónicos enviados por Internet.
- Por otra parte, se verificarán datos como direcciones IP: 181.244.36.251; o message ID: qwXsfwWqNJ; los que necesariamente deberán ser interpretados por un especialista.

PRESERVACIÓN DE EVIDENCIA DIGITAL CADENA DE CUSTODIA

- Es una serie de recaudos destinados a asegurar el origen, la identidad o e integridad de la evidencia, evitando que se pierda, destruya o altere.
- Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria.
- Posibilita controlar la evidencia que contenga datos personales o sensibles.
- Comienza desde el momento del hallazgo o recepción de la evidencia
- Participan todos los funcionarios y o empleados que intervengan durante las etapas del proceso sobre las evidencias.

3

CORRUPCIÓN Y RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA

Binomio pernicioso y necesario de atacar



PGE

Procuraduría General del Estado

Centro de Formación y Capacitación

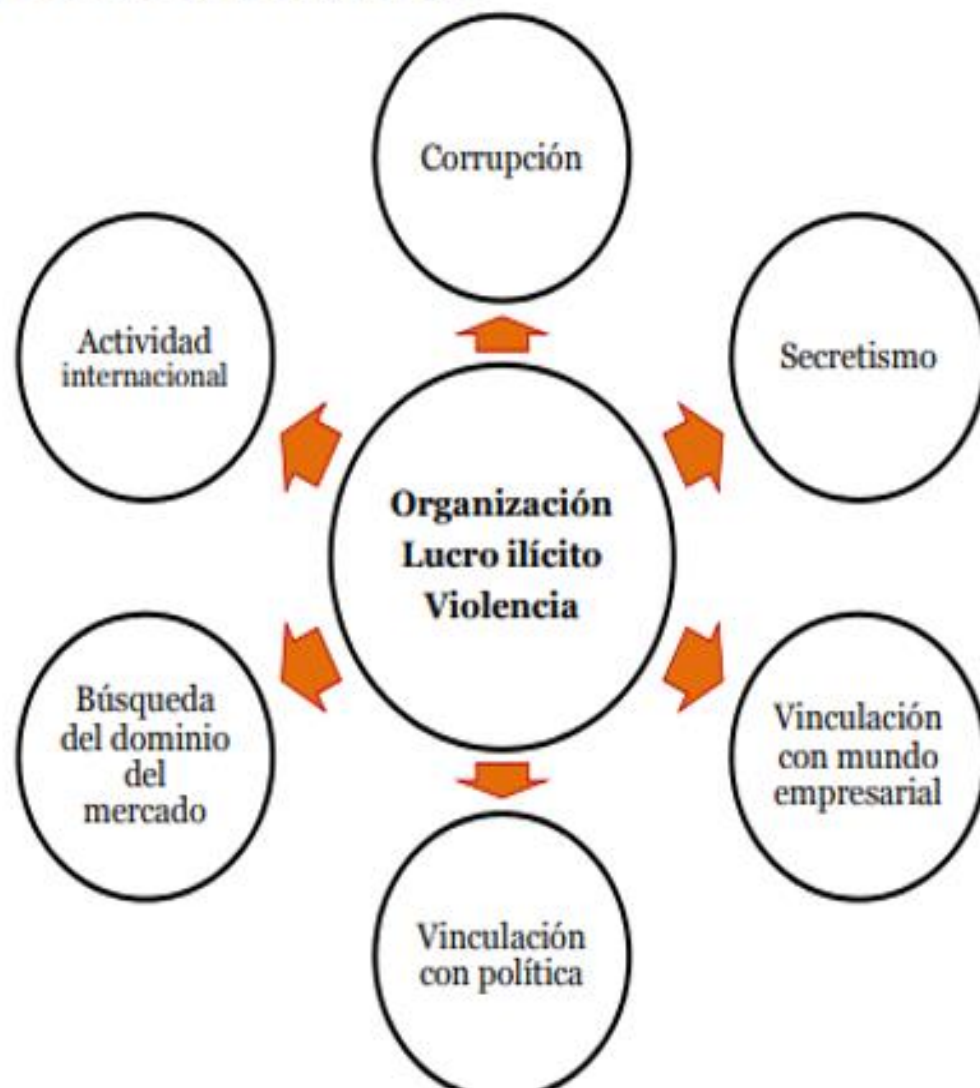


Gobierno del Peru



BICENTENARIO DEL PERÚ 2021 - 2024

B. Elementos accidentales



1ra. Cumbre Internacional de Análisis Criminal Científico
Carabineros de Chile y Centro de Análisis y Modelamiento en Seguridad

**MODELO TEÓRICO PARA LA IDENTIFICACIÓN DE LA
DELINCUENCIA ASOCIATIVA**

ESTUDIO DE CASOS DE CRIMINALIDAD ORGANIZADA A TRAVÉS DEL CINE

26 de Abril de 2014

Maira Nakousi Salas
Daniel Soto Muñoz



PGE

Procuraduría General del
Estado

MUCHAS GRACIAS
