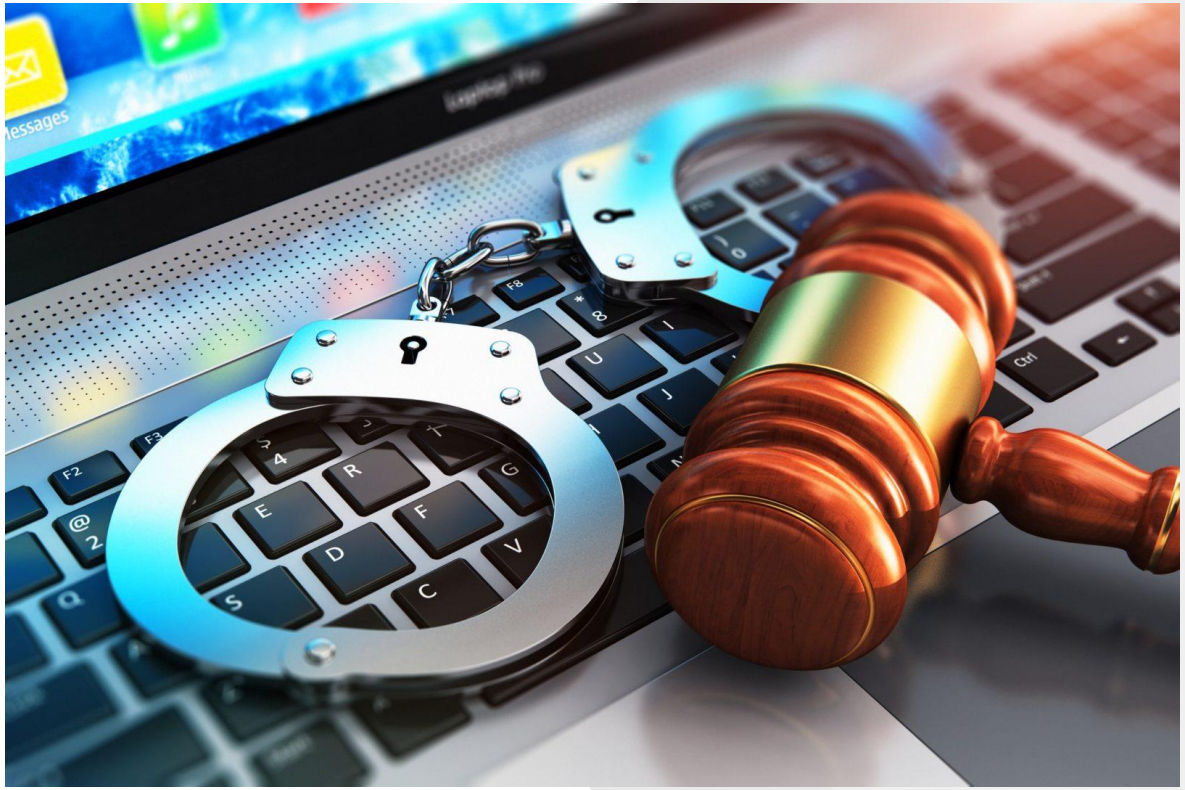
PGE Procuraduría General del Estado

Centro de Formación y Capacitación

Gobierno del Peru

BICENTENARIO DEL PERÚ 2021 - 2024

Delitos contra la intimidad y delitos informáticos Evidencia digital – parte procesal



Mg. Miguel Angel Osco Escobedo

CONTENIDO

PGE
Procuraduría General del Estado

1

Delitos contra la intimidad

Derecho a la Intimidad

- Constitución Política del Perú articulo 2°, inciso 7°
- Declaración Universal de Derechos Humanos articulo 12°
- Pacto Internacional de Derechos Civiles y Políticos articulo 17°
- Convención Americana sobre Derechos Humanos articulo 11° y 14°

Derecho a la Intimidad

Protección de la privacidad como el “derecho al secreto”

Finalidad Fundamental:
Tutelar, la reserva de la persona en cuanto ser psicofísico, sus comunicaciones, sus relaciones afectivas mas cercanas y profundas y la de su hogar, esto es, del lugar donde se desarrolla su vida intima, el espacio en el que se desenvuelve su existencia privada.

→

Alcance:
Substraerse del conocimiento de otra persona, ciertos aspectos de la vida en particular del sujeto, sino también se impone una actividad de prudente distancia, a efectos de no atentar contra costumbres o sentimientos a esa vida intima.

Codigo Penal

Artículo	Delito	Conducta
154	Violación de la intimidad	Observar, registrar, palabra, escrito o imagen íntima
154-A	Trafico ilegal de datos personales	Comercializar información no pública e íntima de otro
154-B	Difusión de imagenes, materiales, audiovisuales o audios con contenido sexual	Publicar o vender contenido sexual obtenido con anuencia de la víctima pero sin su autorización para difundirla
156	Reveleación de la intimidad	Exponer aspectos íntimos confiados en contexto laboral
157	Organización y uso indebido de archivos computarizados	Organiza, proporciona datos sobre convicciones religiosas, políticas u de caracter íntimo

Ley de Delitos Informaticos

La Ley de Delitos Informáticos (Ley 30096) modificada por la Ley Nº 30171, publicada el 10 de marzo del 2014 para adecuar de mejor manera la descripción de sus conductas delictivas al Convenio de Budapest establece cinco grandes grupos de ciberdelitos en función a los bienes jurídicos, a saber, los datos y los sistemas informáticos, la indemnidad y la libertad sexuales, **la intimidad** y el secreto de las comunicaciones, el patrimonio y, por último, la fe pública.

CAPÍTULO IV
DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

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 los supuestos anteriores.

Algunos ejemplos de delitos contra la intimidad

La difusión de imágenes intimas sin el consentimiento de la persona retratada (conocido como porno venganza)

SEXTORSION

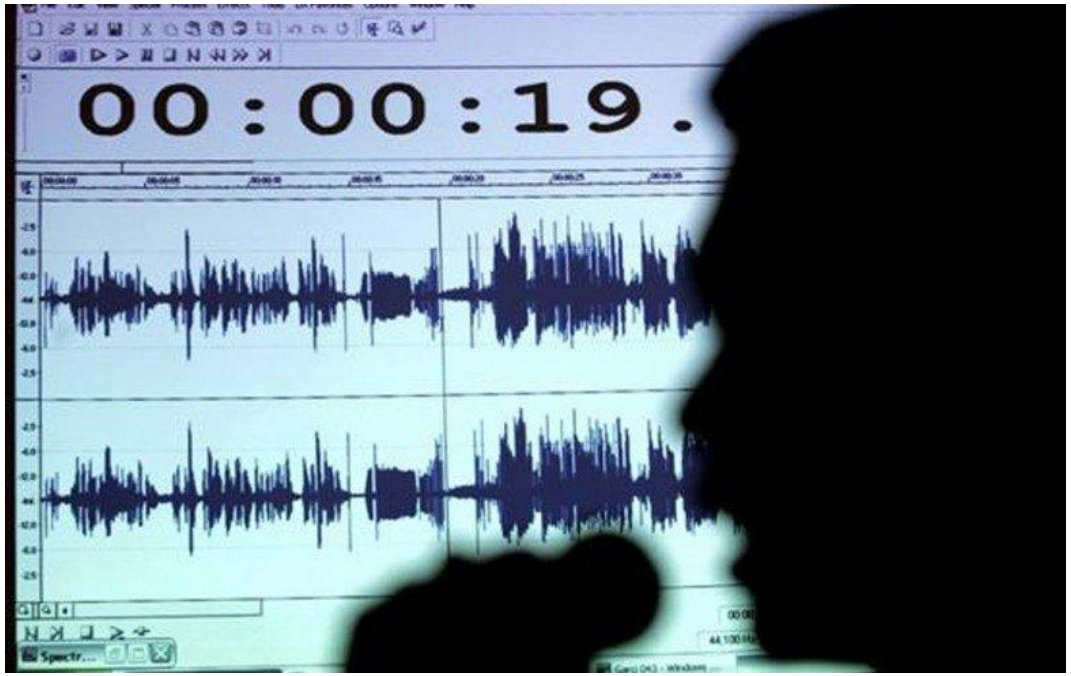
Es una forma de chantaje en la que se amenaza a una persona con divulgar y hacer pública imágenes y videos de su intimidad sexual.

Algunos ejemplos de delitos contra la intimidad

La interceptación y grabación de conversaciones telefónicas o de mensajes de texto sin el consentimiento de las personas involucradas

CHUPONEO

La interceptación ocurre cuando un tercero escucha una conversación telefónica privada, pero también puede hacerse a comunicaciones por correo electrónico o a mensajes de texto enviados por dispositivos móviles o por computadores conectados a redes Wi -Fi.



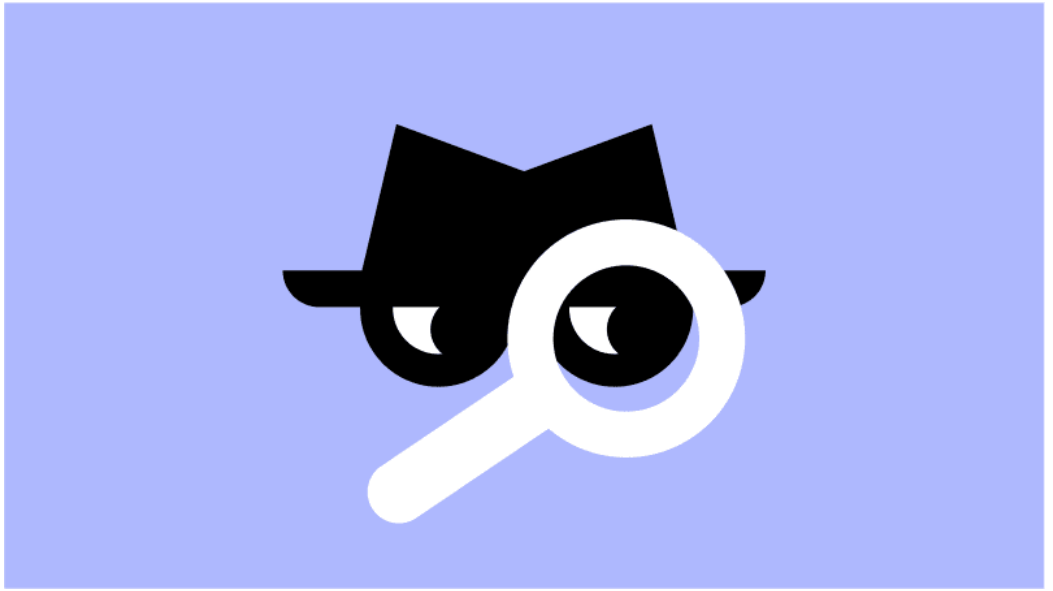
Algunos ejemplos de delitos contra la intimidad

La instalación de cámaras ocultas o la realización de grabaciones sin el consentimiento de las personas involucradas

SPYWARE

Es un software maliciosos diseñado para espiar su actividad en Internet y recopilar datos personales sin su conocimiento o consentimiento. Si no se previene o se detecta, el spyware puede provocar problemas como fraudes y robos de identidad.

«El spyware se ejecuta silenciosamente en segundo plano y recopila información»



Algunos ejemplos de delitos contra la intimidad

La publicación de información privada en línea, como números de teléfono, direcciones de correo electrónico o información bancaria, sin el consentimiento de la persona afectada.

INGENIERIA SOCIAL

Diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios

OSINT

Técnica utilizada en el mundo de la seguridad informática para recopilar información de fuentes públicas y privadas que estén disponibles en línea.

PÉRDIDA DE LA INTIMIDAD EN LA RED |

CONSECUENCIAS Y RIESGOS

La pérdida del control sobre nuestra información personal puede tener ciertas consecuencias :

- Dificultad para eliminar la información :

Es casi imposible hacer que lo que subimos o publicamos en internet sea eliminado y desaparezca completamente. Esto podría generar una gran frustración y también problemas en el futuro.

- Suplantación de identidad y perfiles falsos :

Compartir y publicar cierta información personal puede dar lugar a que alguien la utilice para hacerse pasar por ti, y de esa forma acceder más fácilmente a tus cuentas personales. O simplemente para robar tus fotos y crear perfiles falsos.

- Riesgos para la seguridad personal :

La publicación de información referente a ubicaciones, lugares de ocio habituales, horarios o rutinas facilita que la persona pueda ser localizada físicamente.

- Chantaje y amenazas :

Compartir información, fotos o vídeos sensibles e íntimos podría dar lugar a chantajes, basados en la amenaza de que esa información será publicada si no haces lo que la persona quiera.

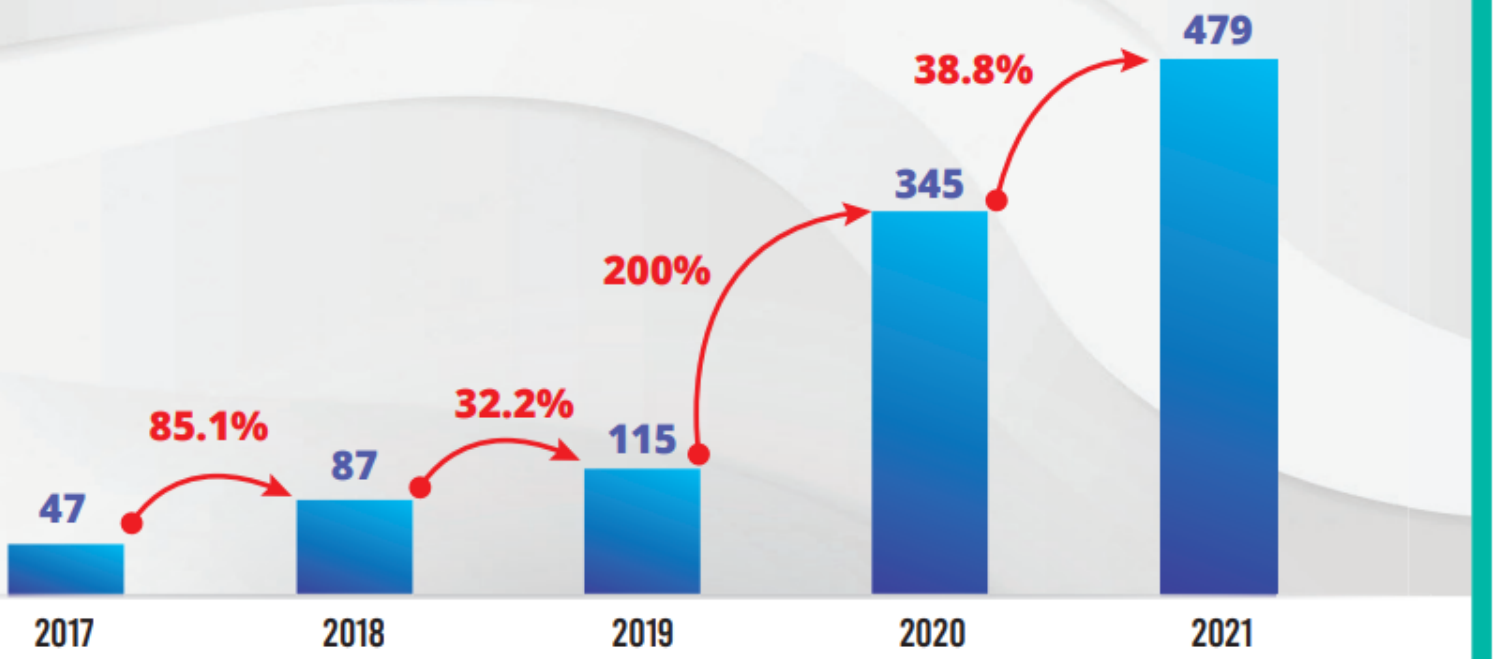
- Posibles destinos de esa información :

La información perdida podría ir a parar a cualquier sitio, como a páginas pornográficas, por ejemplo.

- Acoso personal y Ciberacoso :

La información pérdida podría dar lugar a que esta fuese utilizada en tu contra, para ridiculizarte, insultarte, crear mentiras sobre ti... ya sea personalmente o mediante el ciberacoso.

GRÁFICO 06 Variación porcentual de delitos informáticos contra la intimidad y el secreto de las comunicaciones denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

2

Delitos informáticos

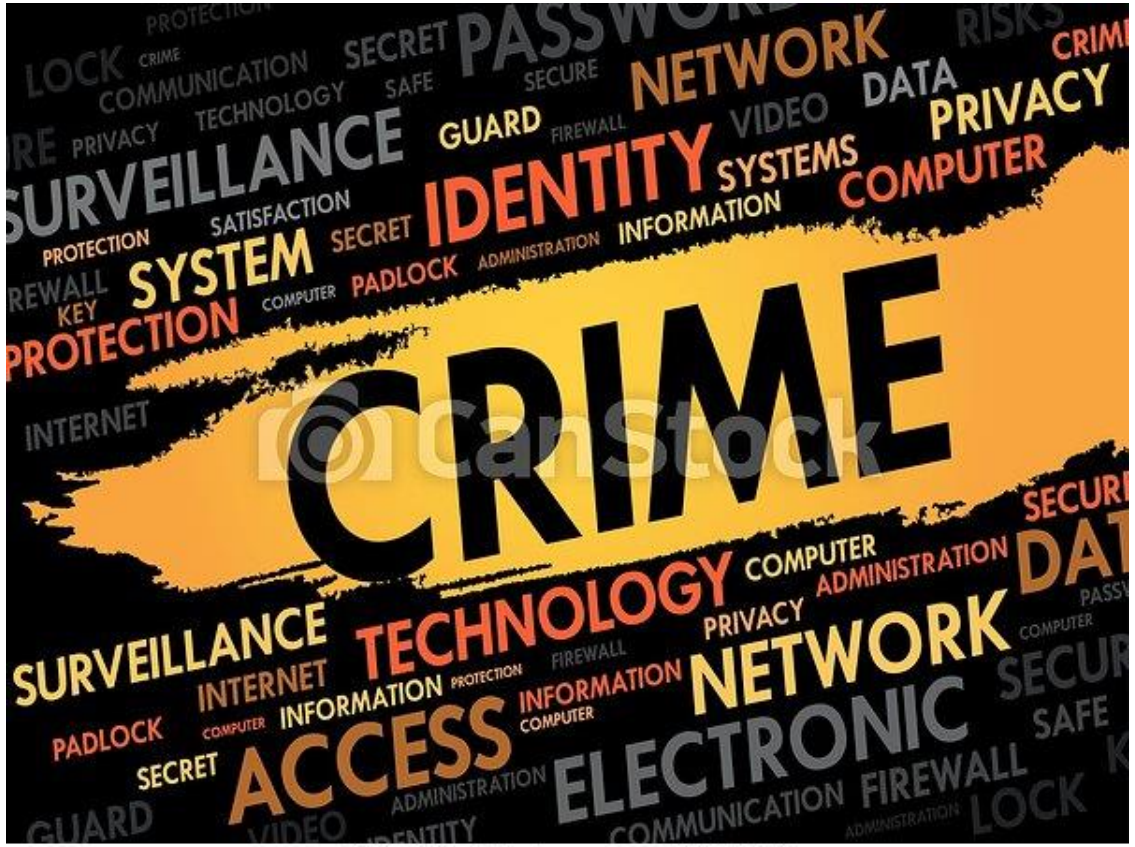
Delitos informáticos

Definición de **delitos informáticos:**

- ✓ No refieren a un tipo de criminalidad específica.
- ✓ Adquieren esta definición a partir del **lugar que ocupa la tecnología** en la comisión del hecho ilícito

Es una definición **instrumental**

- ✓ Conductas antijurídicas e ilegales que utilizan un dispositivo informático como ***medio*** para la comisión de un delito o como ***fin*** del delito mismo.



Definición de **dispositivo informático:**

Dispositivo: aparato o mecanismo capaz de ejecutar una o varias acciones con un fin determinado.
Informática: Conjunción de palabras *"información"* y *"automática"*. Refiere al procesamiento automático de información mediante sistemas electrónicos.

Definición de **dispositivo informático:**

Aparato capaz de procesar automáticamente datos con un fin determinado mediante tres tareas básicas, entrada, procesamiento y salida de información en forma electrónica.

Ejemplos de **dispositivos informáticos:**

- ✓ Computadoras, notebooks, tablets, smartphones, cámaras fotográficas, filmadoras digitales, televisores inteligentes, consolas de videojuegos, entre otros.

¿QUÉ ES UN ARCHIVO EN INFORMÁTICA?

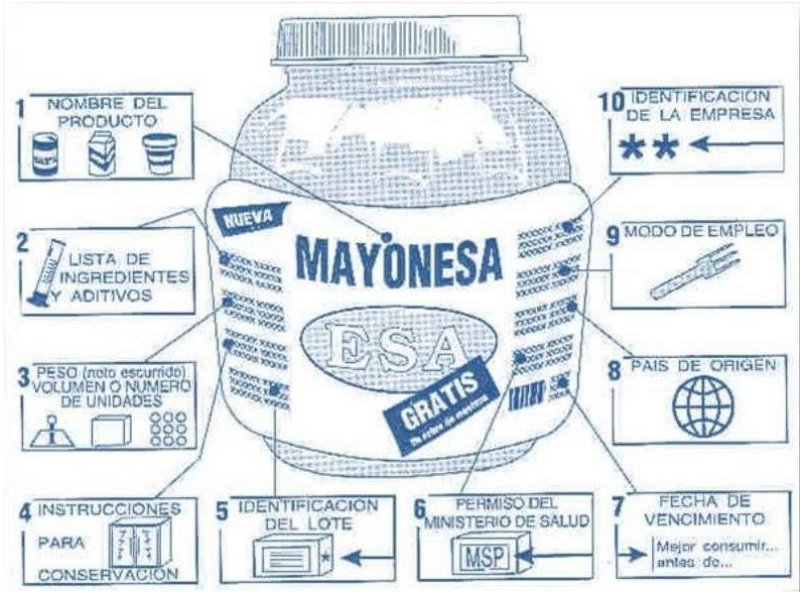
Archivo digital que contiene datos en un formato específico, como una serie de números o texto. La finalidad de estos ficheros es **almacenar, organizar y recuperar datos de forma sistemática**

CARACTERÍSTICAS EN COMÚN

- Nombre
- Extensión
- Tamaño
- Atributo
- Ubicación
- Formato.

BUSQUEDA DE METADATOS

La definición básica de metadatos es “datos sobre datos”. Describen el contenido de algo, el cual no es parte del contenido por si mismo. Por ejemplo en un archivo de video, la longitud del mismo puede ser parte de sus metadatos, pero no es parte del video por si mismo. De manera similar para un archivo de imagen, el fabricante de la cámara utilizada para capturar una foto puede estar en sus metadatos, o la fecha en la cual se capturó la foto, lo cual puede decir algo relacionado a la foto por si misma, pero no es parte del contenido de la foto.



IMAGENES

https://www.thexifer.net/#upload

DOCUMENTOS

https://www.metadata2go.com/

Características de los delitos informáticos que se cometen en Internet

1. Actualmente lo informático constituye no sólo en un medio sino incluso en un objeto potencial para la realización de ilícitos estrictamente cibernéticos.

indispensable a tomar en cuenta es que en este último año se creó la **Unidad Fiscal Especializada en Ciberdelincuencia:**

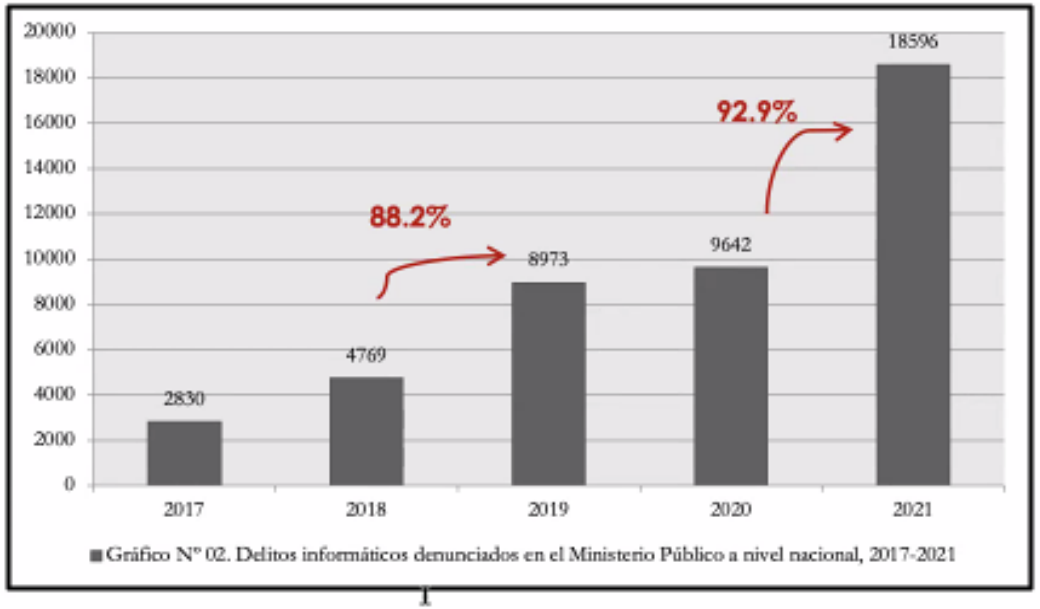


Gráfico N° 02. Delitos informáticos denunciados en el Ministerio Público a nivel nacional, 2017-2021

Fuente: Página 14 del Reporte de información estadística y recomendaciones para la prevención.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**0.1%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

Características de los delitos informáticos que se cometen en Internet

2. Internet es una red mundial que presenta un **alcance global** a la que se puede acceder desde cualquier parte del mundo prácticamente al instante. Ello permite que los potenciales delincuentes puedan actuar desde cualquier lugar del mundo, buscar a las víctimas más vulnerables en cualquier lugar y efectuar los ataques también en y desde cualquier lugar, evitando la persecución gracias a la deslocalización que ofrecen este tipo de actividades cibernéticas.

Características de los delitos informáticos que se cometen en Internet

3. Se ha acrecentado la característica transnacional o transfronteriza de estos delitos, con los consiguientes problemas competenciales entre jurisdicciones de distintos Estados, la disparidad de sus normativas penales en la sanción de una misma conducta, o incluso su consideración o no como delito y la existencia de los llamados "paraísos informáticos", auténticos reinos de impunidad para el delincuente por internet.

CiberSeguridad: Caso Estonia 2007

Estonia es uno de los países más desarrollados tecnológicamente no sólo de Europa sino del mundo.

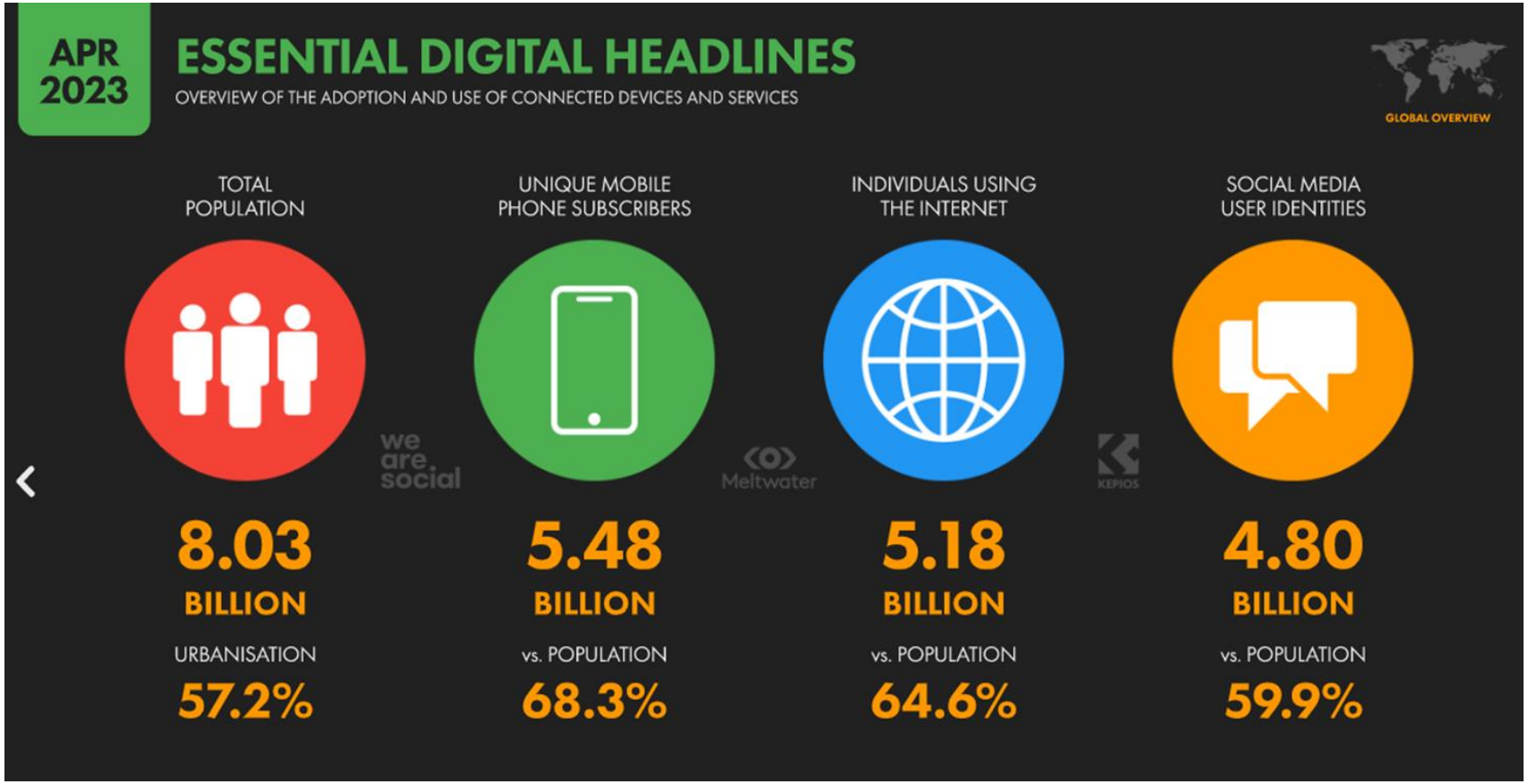
El ataque informático a Estonia marcó un antes y un después en la manera en que se dirigen ataques digitales desde el ciberespacio, nunca antes una nación había sido llevada a un apagón digital por un grupo de hackers.

Los Estonios están muy orgullosos de sus logros tecnológicos y es por esta razón que este ataque informático les dolió tanto.

Inmerso en el estudio de la situación, descubre que la mayoría de peticiones de acceso procedían de Egipto, seguido por Vietnam y Perú –evidentemente no era debido a un repentino interés de los egipcios, vietnamitas o peruanos en la vida social de Estonia o en la lengua estonia–, por lo que decidió cortar la conexión con el extranjero. El ancho de banda se recuperó inmediatamente, el servicio comenzó a funcionar pero sólo en Estonia, el periódico no podía informar al mundo de lo que estaba pasando. Batalla perdida.

Características de los delitos informáticos que se cometen en Internet

4. El gran número de usuarios, las frecuencias de acceso y uso, así como la libre circulación y navegación tanto para emitir, trasferir y difundir información como para acceder a ella por medio de la red, permite que los cibernautas puedan ser al mismo tiempo potenciales víctimas como perpetradores de los hechos ilícitos.



Características de los delitos informáticos que se cometen en Internet

5. Facilita el anonimato, tanto para los delincuentes con conocimientos técnicos que pueden recurrir a la utilización de herramientas para la navegación anónima, como también para aquellos que carecen de esos conocimientos técnicos, pues les otorga cierto y relativo anonimato cuando operan a gran distancia detrás de un número IP, dirección de correo electrónico o perfil, ya que a menudo no es fácil rastrear a un individuo específico.

Características de los delitos informáticos que se cometen en Internet

6. Permite la interacción distante con las víctimas, eliminando posibles barreras sociales que los delincuentes encuentran en la interacción de persona a persona.
   La ciberdelincuencia implica por lo tanto "las relaciones anónimas entre perpetradores y víctimas"

Características de los delitos informáticos que se cometen en Internet

7. Las propias características físicas, técnicas y lógicas facilitan la manipulabilidad de datos y el software con un costo mínimo, ya que se basa en la representación digital (lo que permite la copia sin pérdida de calidad, y la alteración sin huellas visibles). Así, se afirma que *"lo real puede convertirse en falso, el original en copia y el ser en identidad virtual"*.

Características de los delitos informáticos que se cometen en Internet

8. Permite la automatización en la comisión del delito, en aquellos casos en los que un virus es lanzado a internet puede replicar y atacar a millones de ordenadores al mismo tiempo, pero también a lo largo de períodos de tiempo, e incluso personalizarse para crear un nuevo virus.

Características de los delitos informáticos que se cometen en Internet

9. Puede generar un daño de mayor escala y de mayor consideración (por ejemplo, cuando una fotografía es publicada en la red adquiere un alcance global y un impacto mucho mayor que por cualquier otro medio).

Características de los delitos informáticos que se cometen en Internet

10. Puede atacar a diversas víctimas pero ocasionar a cada una de ellas un daño muy pequeño (como por ejemplo, a través de las técnicas por las cuales se sustrae 0,5 céntimos de euro de diez mil cuentas bancarias diferentes mil veces). Este problema de *minimis* puede ser uno de los mayores retos de la ciberdelincuencia ya que reduce los incentivos para informar, investigar y enjuiciar el delito.

Características de los delitos informáticos que se cometen en Internet

11. Facilita o magnifica la comisión de delitos cuyo injusto viene fundamentado en los contenidos de la información, como son los casos de apología del terrorismo, la discriminación de determinados grupos de personas, la xenofobia, la comisión de injurias contra terceros, la difusión de pornografía infantil, la distribución e intercambio no autorizado de obras de creación intelectual etc… Internet no solo facilita la difusión por sus características, sino también debido a que abarata los costes de difusión al tiempo que favorece la comunicación y el intercambio entre personas afines (ej. pornografía infantil).

Características de los delitos informáticos que se cometen en Internet

12. Internet facilita el comercio de la información que se ha convertido en un activo valioso tanto en el mercado legal (música, películas, software, libros) como en el mercado negro, donde los números de tarjetas de crédito, información personal y contraseñas se comercializan para facilitar el fraude y el robo. Incluso se ha convertido internet en un medio a través del cual se realizan acciones de ciberguerra y ciberespionaje.

Características de los delitos informáticos que se cometen en Internet

13. Su innovación constante permite nuevas técnicas y herramientas que se desarrollarán con el objetivo de burlar las medidas de seguridad existentes y cometer nuevos delitos

ASPECTOS PROBLEMÁTICOS

PODER JUDICIA DEL PERÚ

MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN

- ✓ Falta de capacitación y logística en el Ministerio Público, Poder Judicial y PNP.
- ✓ Poco desarrollo doctrinario y jurisprudencial.
- ✓ Conflictos de competencia.
- ✓ Volatilidad de la prueba.
- ✓ Fácil suplantación y falsificación de perfiles en redes sociales.
- ✓ Dificultades en la ubicación de los ciberdelincuentes.
- ✓ Dificultades en la cooperación técnica internacional.
- ✓ Poca colaboración de las empresas operadoras.

Factores que explican el bajo nivel de denuncia:

- ✓ Desconocimiento de los usuarios de que están siendo víctimas de un delito.
- ✓ La ausencia de legislación que tipifique conductas indebidas o hechos ilícitos relacionados con dispositivos informáticos.
- ✓ Baja resolución judicial por falta de capacitación de funcionarios judiciales (jueces, fiscales, peritos).
- ✓ El temor de las empresas a denunciar estos delitos para preservar su imagen y reputación y/o evitar multas o sanciones.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004

Capítulo II - Medidas que deberán adoptarse a nivel nacional

Sección 1 - Derecho penal sustantivo

Título 1– Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integración del sistema, abuso de los dispositivos)

Título 2– Delitos informáticos (falsificación informática, fraude informático)

Título 3– Delitos relacionados con el contenido (pornografía infantil)

Título 4– Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Título 5– Otras formas de responsabilidad y de sanción (tentativa y complicidad, responsabilidad de las personas jurídicas, sanciones y medidas)

Sección 2 – Derecho procesal

Título 1– Disposiciones comunes (ámbito de aplicación de las disposiciones de procedimiento, condiciones y salvaguardias)
Título 2– Conservación rápida de datos informáticos almacenados (y de los datos relativos al tráfico)
Título 3– Orden de presentación
Título 4– Registro y confiscación de datos informáticos almacenados
Título 5– Obtención en tiempo real de datos informáticos (datos relativos al tráfico, interceptación de datos relativos al contenido)

Sección 3 – Jurisdicción

CONVENIO SOBRE CIBERDELINCUENCIA

Aprobado mediante Resolución Legislativa N° 30913, del 12 de febrero de 2019; y, ratificado a través del Decreto Supremo N° 010-2019-RE, del 9 de marzo de 2019. Entrará en vigor el 1 de diciembre de 2019).

Estrasburgo, 12.V.2022

Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia sobre cooperación reforzada y divulgación de pruebas electrónicas

Artículo 7 – Divulgación de la información del suscriptor

1 Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para facultar a sus autoridades competentes a emitir una orden que se presentará directamente a un proveedor de servicios en el territorio de otra Parte, con el fin de obtener la divulgación de la información específica almacenada del suscriptor. en posesión o control de ese proveedor de servicios, donde la información del suscriptor es necesaria para las investigaciones o procedimientos penales específicos de la Parte emisora.

3

Evidencia digital – parte procesal

Definición de la Evidencia Digital

Es todo registro informático almacenado en un dispositivo informático que se transmite a través de una red informática y que puede tener valor probatorio para una investigación.

Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales.

Importancia y tratamiento de la Evidencia Digital

El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas.

Características Técnicas de la Evidencia Digital

DUPLICABLE:

A través de procedimientos forenses el especialista puede generar duplicados de la evidencia digital, los cuales mediante un riguroso registro de cadena de custodia pueden garantizar la continuidad del debido cuidado de esta, su integridad, confidencialidad y disponibilidad. Otra perspectiva de la duplicidad de la evidencia digital la encontramos en la posibilidad de que la interacción de una o más personas a través de un medio informático se almacena de manera simultánea en diferentes repositorios susceptibles en todo caso de ser recolectados y aportados como evidencia digital, como ejemplo, existe la posibilidad de disponer de evidencia almacenada localmente en un dispositivo y paralelamente tener un duplicado en la nube disponible para consulta.

Características Técnicas de la Evidencia Digital

ALTERABLE Y MODIFICABLE:

Dadas sus características técnicas, la evidencia digital puede ser objeto de manipulaciones por parte de terceros si no se respeta el debido cuidado expuesto en el principio de confidencialidad, no obstante, la comunidad técnico científica ha desarrollado procedimientos para validar la integridad e inmodificabilidad de la evidencia al asignarle un valor único alfanumérico que garantiza una identificación que debe permanecer durante el transcurso de la actuación procesal como certeza de que se ha cumplido a cabalidad este propósito.

Características Técnicas de la Evidencia Digital

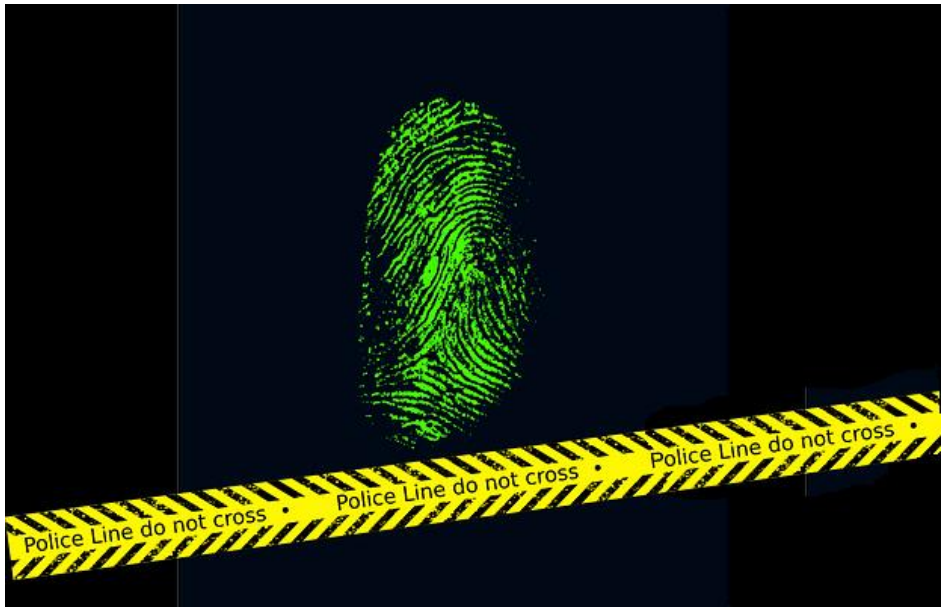
ELIMINABLE:

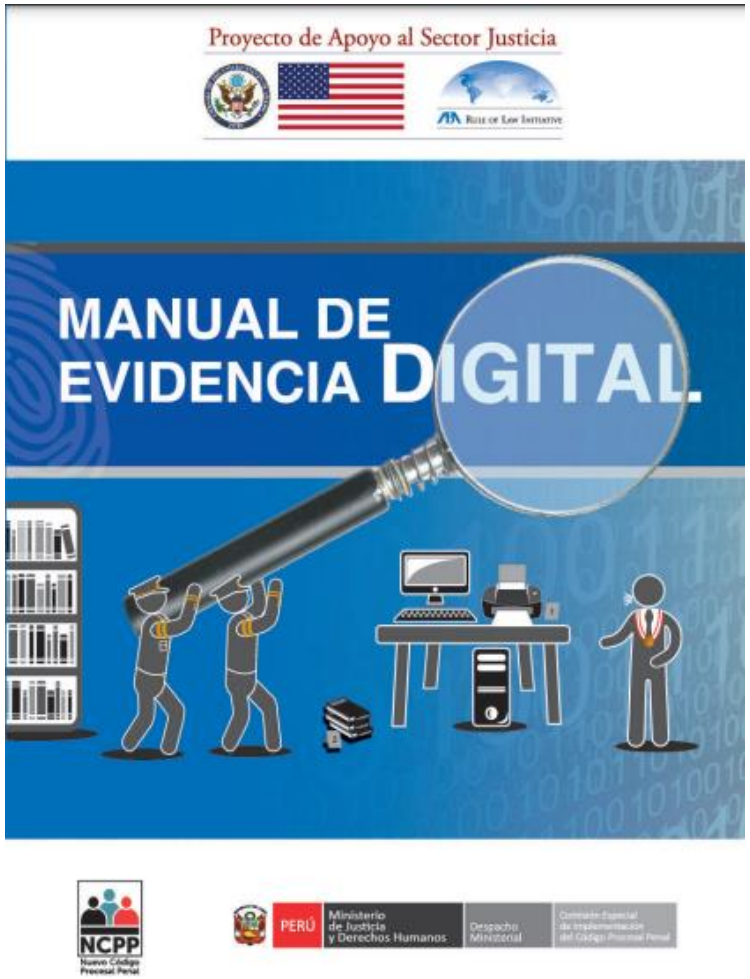
Esta característica señala que la evidencia digital puede ser eliminada por una acción voluntaria o involuntaria de quien la accede, manipula o custodia. La evidencia digital al estar almacenada en un soporte digital y ser generada a través de pulsos electromagnéticos puede eliminarse por una acción deliberada de descargas no deseadas de energía o acción de ondas producidas por un elemento altamente conductor o transmisor de ondas, señales o pulsos que tienen la capacidad de eliminar la originalidad de la evidencia. Igualmente, un transporte inadecuado puede generar daños físicos a los dispositivos de almacenamiento, lo que sin duda puede ocasionar que la evidencia se elimine o se pierda definitivamente.

Características Técnicas de la Evidencia Digital

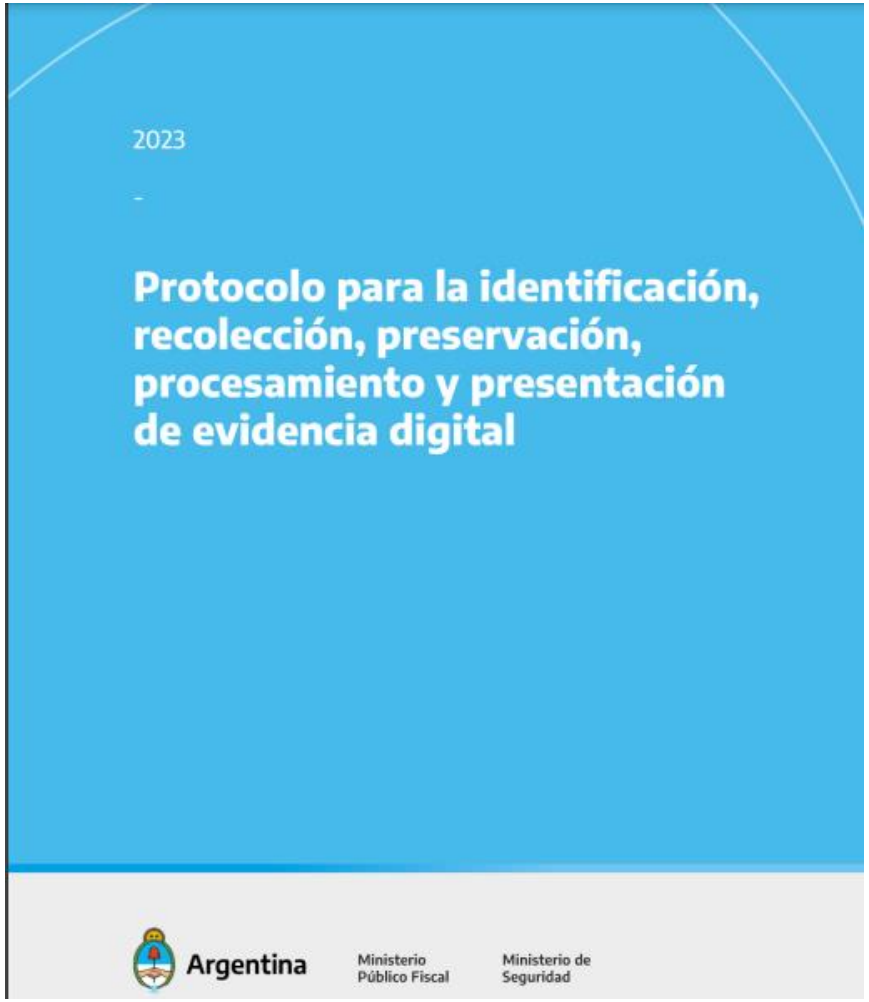
SON ANONIMAS:

La condición de anonimato de la evidencia es una de las características más exigentes en la labor de un especialista forense y por tanto del operador judicial al momento de validar la autenticidad, debido a la difícil tarea de vincular mediante un nexo causal directo a la evidencia digital con el sujeto relacionado con miras a adjudicar una responsabilidad objetiva. Ejemplo de lo anterior, podemos encontrarlo en suplantaciones de perfiles de redes sociales, sin que necesariamente el autor de esta suplantación sea el titular de la red, por ello se hace necesario vincular el actuar de suplantación a una persona determinada.





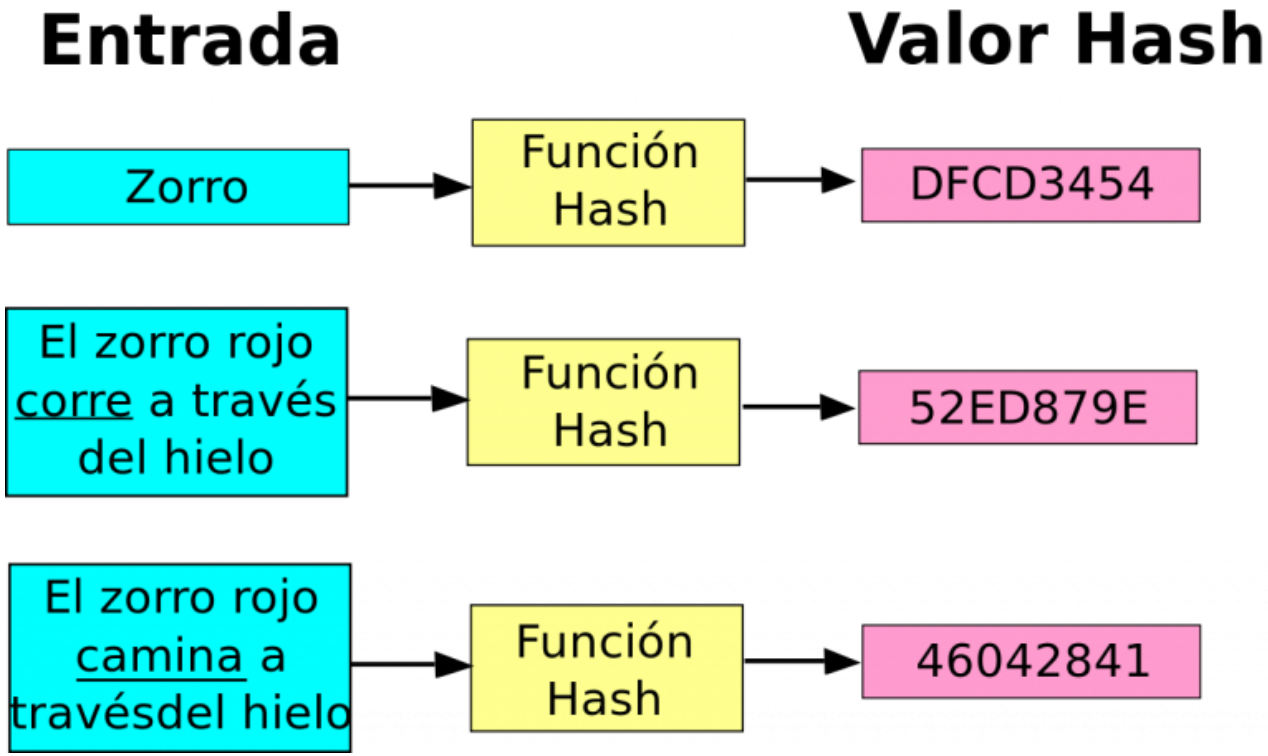
https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf



https://www.diariojudicial.com/public/documentos/000/108/028/000108028.pdf

FUNCIÓN HASH

La “Función Hash” es un algoritmo matemático que codifica unos datos en una serie de carácteres únicos, es decir, es una **función criptográfica**. El “Hash”, por su parte, es el resultado obtenido: **un código alfanumérico único.**



HERRAMIENTA

https://emn178.github.io/online-tools/sha256.html

https://www.pelock.com/products/hash-calculator

PGE

Procuraduría General del Estado

MUCHAS GRACIAS