# CIBERDELITOS

## Guía

Poder Judicial de la Provincia de Salta

# Índice


1. Introducción ..... 5
2.¿Qué son los delitos informáticos o ciberdelitos? ..... 6
3. Menores ..... 8
    Grooming ..... 8
    Pornografía infantil en medios tecnológicos ..... 9
    Corrupción y trata de menores mediante Internet ..... 11
4. Datos Personales ..... 12
5. Daño Informático ..... 14
    Daños informáticos ..... 14
    Virus informáticos / Malware ..... 16
    Difusión de Malware con amenazas, extorsiones y chantajes ..... 17
6. Acceso indebido, intercepción e interrupción de comunicaciones electrónicas y telecomunicaciones. Publicación indebida ..... 18
    Acceso indebido, intercepción e interrupción de ..... 18
    Publicación indebida ..... 19
7. Acceso indebido a un sistema o dato informático ..... 21
8. Propiedad intelectual software ..... 23
9. Fraude y estafa informática ..... 24
    Phishing (Password - Fishing) ..... 24
    Variantes Phishing: Vishing/Smishig ..... 25
    Pharming ..... 25
    Skimming/Clonning ..... 25
    Keylogger (key: tecla, logger: registro) ..... 26
10. Hostigamientos, discriminación, daños al honor, apología del crimen y otros delitos usados mediante componentes informáticos. ..... 27
11. Otras conductas no tipificadas aún como delito en Argentina ..... 28
12. Evidencia Digital ..... 30
13. Evidencia Digital ..... 31
14. ¿Cómo actuar ante un delito informático? ..... 32
15. ¿Dónde denunciar y solicitar asesoramiento? ..... 35
16. Concientización sobre uso responsable de las TIC ..... 37
    Huella Digital ..... 37
    Equipamiento seguro ..... 38
    Navegación segura por Internet ..... 39
    Uso seguro de correos electrónicos ..... 40
    Prevención en las redes sociales ..... 40
    Uso seguro de Smart Phones ..... 41
    Rol de la familia – Padres y menores ..... 42
17. Referencias y fuentes consultadas ..... 43
18. ANEXO - El ABC de la web (Faro Digital) ..... 45
19. Material Audiovisual sugerido ..... 54

# 1. Introducción

El Poder Judicial de la provincia de Salta pone a disposición de la sociedad esta breve guía para informarse acerca de los distintos desafíos que plantea el uso de las herramientas digitales.

Paralalemente a las formas alternativas de comunicación, producto de la universalización de las redes sociales, aparecieron también nuevas formas de delincuencia. Algunas de ellas ya han sido tipificadas en la legislación argentina y otras se encaminan a ser incluídas.

La denominada “Ciudadanía digital” exige compromiso en su ejercicio. Y una parte fundamental es la formación y toma de conciencia de los riesgos que se enfrentan cuando se usan las nuevas tecnologías. El periodismo y los medios de comunicación tienen un rol fundamental, ya que deben garantizar que distintos sectores de la población estén informados y puedan concientizarse acerca de los desafíos que presenta el mundo digital.

# 2.¿Qué son los delitos informáticos o ciberdelitos?

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera.
Si bien no existe una definición propia de "delito informático" con carácter universal, muchos autores han tratado de definirlo en sus obras, en general la siguiente definición resume el concepto en lo siguiente:

**"Aquel que se da con la ayuda de la informática o de técnicas anexas"; o "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de acción criminógena"; o bien: "cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[1]**

*1. Tobares Catalá, G. H. (2010) Delitos Informáticos; Edit. Advocatus. nota 23 de la página 28.*

## 2.1. Clasificación

**Una clasificación de delitos informáticos adoptada por varios países en la Ciudad de Budapest[2] indica:**

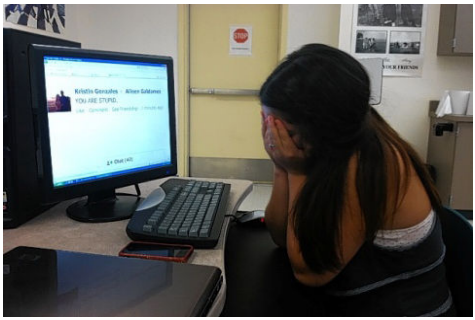
- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.
- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
- Copia y distribución de programas informáticos.
- Piratería informática.

En Argentina, a los delitos ya contemplados en la legislación, mediante la ley 26.388 sancionada en el año 2008, se modificó e incorporó artículos del Código Penal relacionados a delitos informáticos vinculados a pornografía infantil; acceso indebido a correos electrónicos, datos y sistemas; publicación indebida de datos privados; revelación de datos secretos; acceso indebido a datos personales; fraude y estafa informática, distribución de virus (malware); interrupción de comunicaciones; sustracción, alteración, destrucción e inutilización de prueba digital. En el año 2013 se sancionó la ley relacionada con el contacto a menores con el propósito de cometer delitos contra la integridad sexual (Grooming).

*2. Convenio de Cibercriminalidad de Budapest (Hungría), celebrado en Noviembre de 2001.*

# 3. Menores

## 3. 1. Grooming



### 3. 1. 1. Concepto

**"Situación en que un adulto acosa sexualmente a un niño o niña mediante el uso de las TIC. Los perpetradores de este delito suelen generar un perfil falso en una red social, sala de chat, foro, videojuego u otro, donde se hacen pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña que quieren acosar."** (Unicef: Guia de Convivencia Digital).

La Guía de Convivencia Digital (Unicef) **describe dos tipos:**

**1) Sin fase previa de relación y generación de confianza:** El acosador logra tener fotos y videos de los menores mediante la obtención de contraseñas o hackeo de cuentas. El material es obtenido a la fuerza, y el niño o niña acosada puede no saber cómo se obtuvo.

**2) Con fase previa de generación de confianza:** El material es entregado por el menor, y la confianza se vuelve el instrumento indispensable.

Y diferentes fases:
**1) Amistad. Contacto y acercamiento:** El acosador establece contacto a fin de conocer gustos, costumbres y rutinas de los menores. Se vale de herramientas para mentir sobre su edad, mostrando fotos y vídeos falsos o modificados por un programa. El objetivo es mostrarse como un par con quien pueda hablar de temas íntimos.
**2) Relación. Generación de confianza y obtención del material:**
El acosador busca ganar confianza. Para lograr este objetivo, por medio de extensas y continúas conversaciones, se apunta a generar confesiones íntimas y privadas, que pueden más o menos tiempo. El acosador suele logra empatía respecto de los gustos y preferencias de las víctimas. Así consigue el envío del material con componentes sexuales o eróticos.

3) **Componente sexual. Chantaje y Acoso:** El material entregado por el chico o chica se vuelve luego objeto del chantaje, ya sea para la gestación de mayor cantidad de material o bien para lograr un encuentro presencial. Si el menor no accede a sus pretensiones sexuales (más material, videos eróticos o encuentro personal), el ciberacosador lo amenaza con difundir la imagen con mayor carga sexual que haya capturado a través de Internet (plataforma de intercambio de videos, redes sociales, foros u otros) o enviarla a los contactos personales del niño o niña.

- ***Hipervínculos interactivos***

*¿Cómo actuar ante un delito informático? en la página 32*

*¿Dónde denunciar y solicitar asesoramiento? en la página 35*

### 3.1.2. Código Penal

En Argentina, **el Código Penal lo tipifica en el artículo 131**:

> **"Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma."**

## 3.2.- Pornografía infantil en medios tecnológicos

### 3.2.1.- Concepto

**"Según las Naciones Unidas, el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, define la pornografía infantil como: "cualquier representación, por cualquier medio, de un niño participando en actividades sexuales explícitas, sean reales o simuladas, o cualquier representación de las partes sexuales de un niño, cuya característica dominante sea la representación con fines sexuales"**

Debido al avance de las nuevas tecnologías, el acceso y uso de este contenido se ha incrementado por los nuevos dispositivos y servicios relacionados a la comunicación e Internet.

Páginas de Internet, redes peer to peer, redes sociales, mensajería y uso de la Deep Web son medios que están al alcance de todos y con este tipo de contenido.

*Img. 2: Pornografía infantil*

### 3.2.2.- Código Penal

En Argentina, el Código Penal tipifica en el **artículo 128:**

**"Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.**
**Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.**
**Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.**
**Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.**
**Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años."**

- ***Hipervínculos interactivos***

***¿Cómo actuar ante un delito informático? en la página 32***

***¿Dónde denunciar y solicitar asesoramiento? en la página 35***

## 3.3.- Corrupción y trata de menores mediante Internet

### 3.3.1.- ¿De qué se trata?

A fin de capturar a sus víctimas, los abusadores utilizan diversos medios de la tecnología como ser:

- el chat
- las redes sociales
- buscadores de pareja
- ofertas de trabajo por correo electrónico
- sitios de citas
- otros medios de comunicación de Internet.


*Img. 3: Corrupción y trata de menores mediante Internet*

### 3.3.2.- Código Penal

En la Argentina, estos delitos están tipificados en:

**Corrupción de menores:**
Art. 125 del Código Penal (reemplazado por el artículo 5 de la Ley 26.842)

**Trata de personas menores de edad:**
Artículos 145 bis y 145 del Código Penal.

También existe la **Ley 26061** que tiene por objeto la protección integral de los derechos de las niñas, niños y adolescentes que se encuentren en Argentina.

- ***Hipervínculos interactivos***

***¿Cómo actuar ante un delito informático? en la página 32***

***¿Dónde denunciar y solicitar asesoramiento? en la página 35***

# 4. Datos Personales

## 4.1.- Concepto

**“Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”.**

“**Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.”

(Ley 25.326 de Protección de Datos Personales)


*Img. 4 : Datos Personales*

La **ley 25326**, sancionada en el año 2000, indica los principios generales relativo a la protección de los datos personales; derechos de los titulares de datos; usuarios y responsables de archivos, registros y bancos de datos; control; sanciones y acciones de protección de los datos personales.

**En la actualidad, la mayoría de nuestros datos personales se encuentran en la red Internet y de manera online, desde el uso de homebanking, redes sociales, chats, agencia de viajes, compras online, búsquedas de información, reservas áreas, servicios del gobierno, etc. . Esto genera el riesgo de que nuestros datos sean factibles de cualquier acción delictiva informática relacionada al robo, acceso indebido, eliminación y venta de los mismos. El riesgo es mayor si analizamos que muchos de estos bancos de datos no están situados físicamente en nuestro país, sino que están distribuidos en distintos servidores alrededor del mundo, donde cada nación tiene su legislación específica.**

## 4.2.- Código Penal

En Argentina, **el Código Penal tipifica en el artículo 157 bis** lo siguiente:

**"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:**

**1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;**

**2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.**

**3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.**

**Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años."**

# 5. Daño Informático

## 5.1. Daños informáticos

### 5.1.1.- Conceptos

**En términos generales se define "daño informático" a toda lesión o menoscabo causado a un derecho subjetivo o interés legítimo mediante la utilización de medios electrónicos destinados al tratamiento automático de la información y que, concurriendo determinados presupuestos, genera responsabilidad.**

(Sistema Argentino Información Jurídica – Saijº – Delitos Informáticos)

"**Sistema Informático":** Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa".(Convención de Cibercriminalidad de Budapest – Disposiciones Comunes Anteproyecto Ley Delitos Informáticos 26.388).

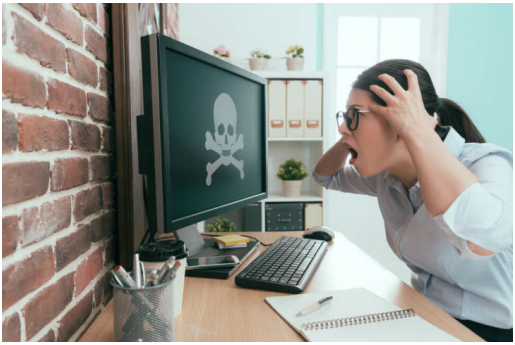
**"Dato informático"**: Toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático. (Convención de Cibercriminalidad de Budapest – Disposiciones Comunes Anteproyecto Ley Delitos Informáticos).

**"Dato informatizado":** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. (artículo 2 Ley 25326 - Protección de Datos Personales).

**"Programa Informático:"** Secuencia ordenada de instrucciones, escritas en un lenguaje de programación, para realizar una tarea específica en una computadora o dispositivo electrónico.

**"Documento:"** Comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. (artículo 1 Ley 26388 Código Penal)

De los conceptos expuestos, existen diferentes delitos relacionados, entre otros, con la destrucción e inutilización de computadoras, celulares, CDs, DVDs, pendrives, cámaras fotográficas u otro dispositivo o medio tecnológico. También el daño de los datos, información y programas ya sea en forma física o por el uso de algún otro programa destinado a causar daños (por ej. un virus informático).



*Img. 5 : Daño informático*

Estas situaciones pueden causar computadoras lentas, borrado de archivos, aumento del tiempo de procesamiento, mensajes falsos y con contenido inapropiado asociados a dañar la imagen de una organización o persona, alteración o destrucción de programas, etc.

En una persona física o jurídica, se pueden generar diferentes situaciones traumáticas no sólo de la pérdida del bien físico sino también en la recuperación, restitución, ratificación, e integridad de los datos y programas que hayan sido afectados.

### 5.1.2.- Código Penal

En Argentina, **el Código Penal tipifica en el artículo 183 segundo párrafo** lo siguiente:

> **"Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno..."**
>
> **En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."**

Cuando el daño es realizado en organismos públicos o relacionados a los servicios de la salud, comunicaciones, provisión o transporte de energía y medios de transporte, las penas se incrementan. **El artículo 184 del Código indica**:

> **"La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:**

**1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;**

**2. Producir infección o contagio en aves u otros animales domésticos;**

**3. Emplear substancias venenosas o corrosivas;**

**4. Cometer el delito en despoblado y en banda;**

**5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;**

**6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."**

## 5.2. Virus informáticos / Malware

### 5.2.1. Concepto

**La Real Academia Española define la palabra "virus informático" como un programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye de forma total o parcial la información almacenada en el disco.** El avance de las tecnologías informáticas dio lugar a otros tipos de programas maliciosos (caballos de troya, macros, bombas lógicas, gusano, exploit, keylogger, crypto, botnet, etc.) destinados a causar daños, sin que ello implique solo su propagación o infección. Estos también permiten tomar el control del sistema operativo, descargar programas y contenidos no autorizados, habilitar el acceso remoto de desconocidos, encriptar archivos, robar datos, capturar la cámara del dispositivo, etc. Por ello actualmente existe un concepto mucho más amplio denominado **"malware" que engloba a cualquier programa potencialmente dañino para el sistema.**

### 5.2.2. Código Penal

En Argentina, el Código Penal tipifica en el artículo. 183 segundo párrafo lo siguiente:

**"Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno..."** En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, **hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."**

## 5.3. Difusión de Malware con amenazas, extorsiones y chantajes

### 5.3.1. Concepto

Por otro lado existen otras figuras delictivas asociadas a la distribución de malware. Estas tienen que ver con el hecho de que, luego de haberse producido la inserción del programa y/o infección de los archivos, los autores o distribuidores de/los mismos extorsionan a los dueños de los datos afectados, solicitando una recompensa económica asociada a la recuperación o restauración a su estado original anterior al hecho. Este tipo de malware son comúnmente denominados "ransomware" (del inglés ransom, 'rescate', y ware, por software) y su metodología fue ampliada difundida por los medios nacionales e internacionales en el último Cyberataque mundial acontecido el día Viernes 12 de Mayo de 2017, donde miles de computadores fueron afectadas.

- *Hipervínculos interactivos*

*¿Cómo actuar ante un delito informático? en la página 32*

*¿Dónde denunciar y solicitar asesoramiento? en la página 35*

### 5.3.2. Código Penal

Esta conducta está **tipificada en el artículo 168 del Código Penal** que indica:

**" Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos."**

# 6. Acceso indebido, intercepción e interrupción de comunicaciones electrónicas y telecomunicaciones. Publicación indebida

**Comunicación electrónica:** Comunicación que las partes hagan por medio de mensajes de datos.

**Mensaje de Datos:** Información generada , enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos, el correo electrónico, redes sociales, chats."
(Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales)

**Telecomunicación:** "Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos."

(Constitución de la Unión Internacional de Telecomunicaciones) (Ginebra, 1992) (CS 1012) (y RR S1.3)

## 6.1. Acceso indebido, intercepción e interrupción de comunicaciones electrónicas y telecomunicaciones

Las acciones delictivas sobre las comunicaciones electrónicas y telecomunicaciones tienen que ver, entre otras, con el acceso ilegitimo de correos electrónicos, chats, redes sociales, radios, teléfonos, televisión, robo de líneas, desvío de tráfico, ataques masivos del tipo spam (correo basura), de denegaciones de servicio (dejar un servicio o recurso inaccesible a los usuarios); espionaje gubernamental, empresarial o político. Esto genera prejuicios a una persona física jurídica, como ser la suplantación de identidad, exposición, caídas del servicio, revelación de datos personales, privacidad, fraude y difamación.

### 6.1.2. Código Penal

**La ley 26.388, modifica e incorpora en los artículos 153 y 197 del Código Penal**, delitos relacionados a las comunicaciones electrónicas y telecomunicaciones:

**"Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.**

**En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.**

**La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.**

**Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena."**

**"Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida."**

## 6.2. Publicación indebida

Otro hecho que se plantea con las comunicaciones electrónicas, tiene que ver con la publicación indebida. En muchas ocasiones, diferentes personas reciben en forma lícita información concerniente solo a las partes que participan de una comunicación electrónica. Casos típicos de un correo electrónico recibido, mensaje de Whatsapp, de texto, mensaje privado de una red social, etc. En virtud de obtener alguna repercusión mediática, interés económico, beneficio personal o ánimos de causar daño, esta información es enviada a terceros generando un perjuicio a la parte remitente de la comunicación.

### 6.2.2. Código Penal

Este tipo de delitos está contemplado **en el artículo 155 del Código Penal** que indica:

**"Será reprimido con multa desde pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.**

**Está exento el que hubiere obrado con propósito inequívoco de proteger un interés público"**

También está contemplado en el Código Penal el delito de publicación o revelación, por parte de un funcionario público, de datos que por ley deben ser secretos. Corresponde a estos datos, los que conoce por la función que cumple dentro de la Administración pública y que es indebidamente difundido. Se trata de una acción por la que el secreto trasciende el ámbito al cual pertenece.

**La tipificación es realizada en el artículo 157 del Código Penal:**

**"Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos."**

**Cuya pena puede ser mayor, cuando el delito esté relacionado a una conducta más específica y citada en el artículo 222 del Código Penal**:

**"Será reprimido con reclusión o prisión de uno (1) a seis (6) años, el que revelare secretos políticos, industriales, tecnológicos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación. "**

- ***Hipervínculos interactivos***

***¿Cómo actuar ante un delito informático? en la página 32***

***¿Dónde denunciar y solicitar asesoramiento? en la página 35***

# 7. Acceso indebido a un sistema o dato informático


*Img. 6 : Acceso indebido a un sistema o dato informático*

## 7.1. Conceptos

Los conceptos relacionados con los accesos indebidos a un sistema o dato informático están vinculados siempre a un sujeto activo denominado "hacker". Si bien la Real Academia Española lo define como "pirata informático: persona con grandes habilidades en el manejo de ordenadores, que utiliza sus conocimientos para acceder ilegalmente a sistemas o redes ajenos"; **en el mundo de la seguridad informática el "hacker" es conocido por sus habilidades para analizar, testear y comprobar vulnerabilidades de seguridad sin producir ningún daño en los datos ni en el sistema en cuanto a su integridad, disponibilidad y confidencialidad**. En cambio se conoce, en el ámbito de la seguridad informática, otra categoría de personas que si realizan acciones maliciosas sobre los sistemas que vulneran.
Entre ellos se puede citar a:

- **Black Hat Hackers (hackers de sombrero negro)/ Crackers:** Rompen la seguridad de una red o computadora o crean virus informáticos. Tienen el objetivo principal de realizar un acceso indebido a fin de causar daños, ya sea robando información, dejando algún virus, malware en el sistema y crean puertas traseras para poder entrar nuevamente. También diseñan programas para romper seguridades del software. Su motivación es el dinero.
- **Gray Hat Hackers (hacker de sombrero gris):** Los que juegan de un lado y otro. Ofrecen sus servicios a empresas o delincuentes. Tienen una ética ambigua entre lo bueno y lo malo.

- **Hacktivistas:** Tienen un fin político o religioso, reivindicativos de derechos, o quejas de la sociedad en general. Trabajan en grupo. El más conocido es Anonymous.
- **Ciberterroristas:** Orientados a vulnerar sistemas con el fin de generar terror o miedo generalizado en una población, clase dirigente o gobierno.
- **Script Kiddies:** Utilizan programas escritos de otros crackers para penetrar algún sistema, red de computadora, página web, etc. Por lo general tienen muchos menos conocimientos que los anteriores.
- **Phreaker:** Con conocimientos para vulnerar sistemas telefónicos como telefonía móvil, inalámbricos y de voz y el Voz sobre IP (VoIP). Sus objetivos pueden ser solamente por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio económico, como llamadas gratuitas.
- **Carders:** Expertos en redes informáticas. Sus ataques son dirigidos a estos tipos de infraestructura.
- **Newbie/Lammers:** Con muy pocos conocimientos. El riesgo siempre está asociado a que no saben realmente que están realizando. Pocas veces logrando penetrar algún sistema vulnerable. Son las categorías más bajas en la trastienda del mundo de los Crackers.

## 7.2. Código Penal

La tipificación de estos delitos están  es realizada en el **artículo 157 del Código Penal:**

**“Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.**

**La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. “**

- ***Hipervínculos interactivos***

*¿Cómo actuar ante un delito informático? en la página 32*

*¿Dónde denunciar y solicitar asesoramiento? en la página 35*

# 8. Propiedad intelectual software


*Img. 7 : Acceso indebido a un sistema o dato informático*

Antes de la sanción de la ley 25.036 (1998) que modifica artículos de la ley 11.723, los delitos relacionados con la propiedad intelectual del software no estaban tipificados. Las copias parciales y totales no autorizadas (piratería), distribución sin consentimiento del autor y ventas ilegales por diferentes medios de Internet y medios magnéticos (CD/DVDs, pendrives, etc.) eran conductas no reguladas y carecían de la protección jurídica del software. La **ley 25.036** sancionada en Octubre/1998 de Protección Jurídica del Software modifica algunos arts. de la ley 11.723 que protege los Derechos de Autor de obras científicas, literarias, artísticas, comprendiendo escritos de toda naturaleza entre ellos los **programas de computación, la compilación de datos u otros materiales sea cual fuere el procedimiento de reproducción.**

Entre los puntos más destacados están:

- De los programas de computación solo se pueden reproducir una copia de salvaguarda que será debidamente identificada (artículo 9).

- Son titulares del derecho de la propiedad intelectual:
  - El autor de la obra.
  - Sus herederos.
  - Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.
  - Las personas físicas o jurídicas **cuyos dependientes contratados** para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

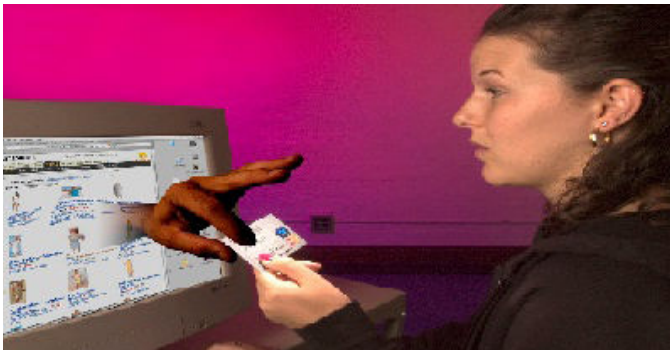
- El artículo 71 refiere a la aplicación del **artículo 172 del Código Penal** que defraudare los Derechos de Propiedad Intelectual.

- El artículo 72 impone además de las penas, el secuestro de la edición ilícita y enumera los casos especiales de defraudación.

Las penas se extienden a quien: edite, venda o reproduzca software ilegal.
• Las personas físicas o jurídicas **cuyos dependientes contratados** para elaborar un programa de computación hubiesen producido un progra ma de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

# 9. Fraude y estafa informática

Las conductas relacionadas a la defraudación y estafa informática corresponden a todas las acciones delictivas derivadas de metodologías asociadas a los conceptos de Phishing, Vishing, Smishing, Pharming, Skiming/Clonnig, etc; como a cualquier otra conducta orientada a modificar, alterar, ocultar y/o manipular datos, sistemas y programas informáticos con un fin delictivo.



*Img. 8 : Fraude y estafa informática*

## 9.1. Acciones delictivas derivadas:

### 9.1.1. Phishing (Password - Fishing)

Es una forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo) a una o varias personas, intentando convencerlas para que revelen sus datos personales mediante la contestación de un correo electrónico o a través de un link en el mismo cuerpo del mensaje. Usualmente, esta información es luego utilizada para realizar acciones fraudulentas, como transferencias de fondos de su cuenta bancaria, compras con sus tarjetas de crédito u otras acciones delictivas que pueden efectuarse mediante la utilización de esos datos.

### 9.1.2. Variantes Phishing: Vishing/Smishig

Al concepto anteriormente mencionado se lo conoce, en el ámbito de la seguridad informática, con otras variantes:
**Vishing**: No indica un link donde ingresar, sino ofrece un número de teléfono donde comunicarse. Por supuesto el número es falso y no corresponde a la entidad que están falseando.
**Smishing**: El medio de comunicación es por llegada de un mensaje de texto, donde generalmente indica un falso mensaje del acreedor de un premio o sorteo e informa un número telefónico para comunicarse.

### 9.1.3. Pharming

Constituye otra forma de fraude en línea, muy similar al phishing. Los pharmers (los autores de los fraudes basados en esta técnica del pharming) atacan la red y equipos de los usuarios modificando y redirigiendo el tráfico a otros sitios fraudulentos. Con ello utilizan los mismos sitios Web falsos y el robo de información confidencial para perpetrar estafas en línea, pero, en muchos sentidos, es mucho más difícil detectarlos, ya no necesitan que la víctima acepte un mensaje "señuelo".

En lugar de depender por completo de que los usuarios hagan clic en los vínculos engañosos que se incluyen en mensajes de correo electrónico falsos, el pharming redirige a sus víctimas al sitio Web falso, incluso si escriben correctamente la dirección Web de su banco o de otro servicio en línea en el explorador de Internet.

### 9.1.4. Skimming/Clonning

Consiste en la clonación de tarjetas de crédito y débitos. El dispositivo "skimmer" permite leer y almacenar los datos de las tarjetas para su copia en otra tarjeta física o para operar con ella en lugares donde no se requiere la presentación del medio físico (por ej. compra online). Este aparato diminuto puede estar instalado y oculto en cualquier cajero manipulado de un Banco, como así también en cualquier lugar físico donde realizamos compras o pagos con la tarjeta. Con ello los delincuentes capturan los datos de la tarjeta (nombre, número de tarjeta, fecha de expiración, código de seguridad, etc.) y con ello pueden realizar compras online en diversos sitios de Internet. Las modalidades de extracciones de dinero se deben complementar con el robo del pin de acceso. Esto lo realizan, instalando en el cajero una cámara de video pequeña e imperceptible que capturan lo ingresado en el teclado. Con los datos de la tarjeta clonada y el pin solo resta conocer el DNI de la persona para realizar la extracción. Este dato es muy fácil de conseguir con cualquier búsqueda en sitios de Internet como Afip, Rentas, padrones electorales o red social.

### 9.1.5. Keylogger (key: tecla, logger: registro)

Programa o hardware que registra y almacena todas las teclas presionadas o pulsadas en un teclado de un dispositivo electrónico (computadora, celular, smartv, etc.). Suele usarse para capturar datos privados de accesos a diversos sistemas y/o aplicativos, como ser usuario y contraseña de un Home Banking, números de tarjetas de crédito, clave fiscal, usuario y contraseña de un sistema, clave de un correo electrónico entre otros. Actualmente han evolucionado y también permiten capturar movimientos del mouse.

## 9.2. Código Penal

En cuanto a la legislación argentina y las tarjetas bancarias, **la ley 25065** establece normas que regulan diversos aspectos vinculados con el sistema de Tarjetas de Crédito, Compra y Débito; las relaciones entre el emisor y titular o usuario y entre el emisor y proveedor y Disposiciones Comunes.

"**Artículo 172.**- Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño."

"**Artículo 173 Inc. 15.**- El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática."

"**Artículo 173 Inc. 16**.- El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"

"**Artículo 162, 164**.- Delitos de robo o hurto"

"**Artículo 282, 283 y 285.**- Falsificación o alteración de moneda"

"**Artículo 175 Inc. 1**.- Apropiación de cosa perdida"

- ***Hipervínculos interactivos***

***¿Cómo actuar ante un delito informático? en la página 32***

***¿Dónde denunciar y solicitar asesoramiento? en la página 35***

# 10. Hostigamientos, discriminación, daños al honor, apología del crimen y otros delitos usados mediante componentes informáticos.

*Img. 9 : Hostigamientos y otros delitos informáticos*

Estos tipos de delitos también pueden ser realizados mediante el uso de los servicios de Internet como ser a través de las redes sociales (facebook, twitter, instagram, etc.), publicaciones en páginas web, correos electrónicos, mensajería (whatsapp, skype, Line, Chaton, etc.) o mediante el uso de cualquier dispositivo electrónico.

**La evidencia digital, correspondiente al uso de estos servicios, puede ser factible de usarse como prueba.**

## 10.2. Código Penal

En Argentina, estos delitos están tipificados en:

- **Falsificación de documentos:** artículo 292 Código Penal.
- **Calumnias e imputaciones falsas de un delito:** artículo 109 (calumnias o imputaciones falsas de un delito) y artículo 110 (injurias) del Código Penal.
- **Intimidación Pública:** artículo 211 Código Penal
- **Discriminación:** Ley 23.592.
- **Apología de un delito, instigación al suicidio y a la violencia:** artículo 83, 209, 212 y 213 del Código Penal.
- **Amenazas:** artículo 149 bis Código Penal.
- **Extorsión:** artículo 168 Código Penal.

## 11. Otras conductas no tipificadas aún como delito en Argentina

A continuación se enumeran algunas conductas delictivas relacionadas con la informática, aún no tipificadas en el Código Penal:

- **Usurpación, robo y/o suplantación de identidad digital:** No está considerado como delito hacerse pasar por otra persona en un blog, en una red social ni en cualquier otro medio electrónico.

- **Acción coordinada de ciberejercitos de tendencia:** Acciones coordinadas y realizadas en redes sociales, blogs, sitios de opinión, comentarios en periódicos online y todo portal pasible de dejar un comentario u opinión; a fin de opinar, comentar, retrucar, difamar o glorificar una o grupo de personas determinadas que reciben lineamientos editoriales de quien los contrata. Entre sus objetivos principales están lo de desinformar o tergivesar la información online con el objeto de generar una tendencia de opinión. En algunas ocasiones son denominados ejército de Trolls.

- **Porno venganza/Sexting:** Publicación o difusión por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas.

- **Violación a la intimidad:** Si bien existen delitos penales relacionados con accesos indebidos de datos y hackeo; la acción de violación a la intimidad solo está contemplada en el artículo 1770 del Código Civil y Comercial.

- **Daño al honor en Internet:** No existe el "derecho al olvido", legislación presente en otros países que permite un mecanismo fácil y rápido para poder quitar, de los resultados de búsqueda, contenidos hechos con la intención de causar un perjuicio

- **Responsabilidad de las compañías tecnológicas:** No está contemplada en la legislación la responsabilidad de las empresas, que proveen buscadores en Internet o sitios que reproducen contenido, respecto de la información que se publica por parte de los usuarios.

- **Abuso de los dispositivos:** No está tipificada la producción, venta, importación, difusión u otra forma de puesta a disposición de dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de delitos.

- **Hurto informático:** La tipificación de apoderamiento ilegítimo hace referencia solo a cosas muebles. En el caso del software, datos y Bases de Datos no personales son bienes intangibles.

- **Captación o venta ilegítima de datos:** Si bien se mencionó el comportamiento asociado a los keylogger y el Phishing con sus modalidades, solo en los casos mediante los cuales se produzcan delitos relacionados con el fraude, hurto de cosa mueble, falsificación o alteración de moneda y apropiación de cosa perdida está tipificado en el código Penal. Las acciones relacionadas con obtener, captar, vender y enviar datos personales, financiaros o confidenciales no están tipificadas.

# 12. Evidencia Digital

## 12.1. Concepto

**La evidencia digital es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectadas y analizadas con herramientas y técnicas especiales.**[3]

## 12.2. Características

La evidencia digital contiene algunas características propias que la distinguen de cualquier otra evidencia tradicional.
Entre otras, contiene las siguientes particularidades:

- **Volátil:** Puede perderse si no se recolecta en tiempo y forma.
- **Duplicable:** Pueden realizarse diversas copias sin poder reconocer el original.
- **Alterable:** Factible de su modificación y/o borrado y sin el registro de esas acciones.
- **Anónima:** En algunos casos no se pueden determinar el autor de las mismas.
- **Posee datos adicionales no visibles por las herramientas tradicionales usadas por el usuario:** Ultimo acceso, modelos de cámara usados en una fotografía, coordenadas de geo posicionamiento, autor, última impresión, secuencia de recorrido de un correo electrónico, etc.).

**Su recolección, preservación y presentación involucra una serie de procedimientos a cumplir en tiempo y forma, a fin de mantener la integridad, autenticidad, confiablidad y validez legal de la misma.**

*Img. 10 : Evidencia digital*

*3. El rastro Digital del Delito (Universidad Fasta - Di Iorio, Constanzo, Curti y otros). Página 80*

# 13. Evidencia Digital

## 13.1 ¿Dónde se puede encontrar?

La evidencia digital puede estar almacenada y activa en cualquier dispositivo electrónico. Entre ellos:

- Computadoras de escritorio.
- Computadoras  móviles.
- Servidores.
- Hardware de red.
- Celulares.
- GPS.
- Cámaras fotográficas.
- Pendrive.
- Memorias flash/Sdcards.
- Impresora.
- Discos rígidos.
- Cd/disquetes/DVD/Cintas magnéticas.
- Sistemas de automóviles.
- Videojuegos.
- Videocámaras.
- Smart TV.

Donde puede existir evidencia relacionada en/con:

- Historial de navegación en Internet.
- Chats de redes sociales y/o aplicación que lo posea.
- Archivos existentes y eliminados (documentos, fotos, videos, planillas, etc.)
- Actividad del usuario en el dispositivo.
- Encendido y apagado de un equipo.
- Aplicaciones instaladas.
- Procesos en memoria.
- Contactos/Llamadas entrantes y salientes/SMS/Mensajes de aplicaciones.
- Cuentas de usuario/contraseñas.
- Correos electrónicos.
- Descargas efectuadas.
- Historial de conexiones de medios removibles.
- Eventos del sistema operativo.
- Base de datos.
- Tráfico de red y su interpretación.
- Conexiones a redes Wifi.

# 14. ¿Cómo actuar ante un delito informático?

## 14.1 Recomendaciones generales

- Si en la situación está involucrado un menor, éste debe contactar e informar a los padres, adulto familiar o directivo responsable, del lugar que se encuentre, de forma inmediata.
- Buscar asesoramiento legal y/o la participación de un perito informático, organización local a fin de que le indiquen que pasos a seguir y como documentar la evidencia que considere pertinente para realizar la denuncia . En el caso de no poseerlo, se sugiere seguir estos pasos:

  • En lo posible no apagar el dispositivo electrónico.

  • No modificar, ni alterar ni realizar ninguna configuración de su dispositivo hasta tanto realice la denuncia.

  • Tratar de documentar y guardar toda la evidencia posible a través de capturas de pantallas, fotografías o videos afines a la situación. Si es posible y tiene los medios, certifique las operaciones y el escenario con un escribano.

- Realizar la denuncia correspondiente acompañando toda la evidencia en la fiscalía más próxima a su domicilio o en la depencia policial de su jurisdicción.
- Luego de realizar la denuncia, cambiar todas las claves relacionados a las cuentas de correo electrónico, redes sociales, acceso al dispositivo, Homebanking y de cualquier otro servicio de internet usado en el dispositivo; ya que es posible que éstas hayan sido accedidas mediante algún malware instalado por el acceso al servicio que se está ingresando u otorgadas por la víctima.

## 14.2. Recomendaciones especiales (adicionales a las generales)

**Grooming:**

- No cierre ni elimine las comunicaciones, foros, chats y cualquier otra operación en la que está participando el menor con el acosador.
- Si la justicia no indica lo contrario, denunciar al perfil del acosador en el lugar (red social, foro, chat) donde la menor se contactó a fin de prevenir el acoso a otros niños/as.

**Pornografía infantil:**

- No publicar el enlace con contenido pedófilo por ningún medio.
- Si es posible y tiene el conocimiento, detecte y documente la existencia de programas relacionados a navegación por la deep web y redes peer to peer.
- Si la justicia no indica lo contrario, denunciar al/las páginas Webs a organizaciones que luchan contra este tipo de personas.

**Sospecha o indicios de virus/malware informático:**

Este último tiene características propias que puede detectar si:

- El navegador web se torna muy lento o no responde, se cambia la página de inicio, se abren sitios web no solicitados y numerosos mensajes emergentes y aparecen barras de herramientas extrañas o inexplicables en la parte superior.
- La pc está más lenta o no responde, se reinicia, aparecen nuevos mensajes o íconos en el escritorio, mensajes de error y no puede acceder a opciones de administración.
- Se recibe correos electrónicos sin remitente o sin asunto, se crean mensajes enviados no realizados, se reciben diversos correos de remitentes desconocidos.

**Si presenta algunas de esas características debe:**

- Realizar una copia de cualquier archivo valioso o importante que se encuentre en su equipo.
- Si existe un antivirus instalado, actualizarlo y luego utilizar la opción “Scanear” o “Examinar” o”Analizar” equipo. Seguir las instrucciones que indica el antivirus para borrar la infección.
- No ejecutar ningún programa ni abrir ningún documento.
- Desconectar Internet.
- Si la infección es proveniente de un ransomware (secuestra los datos y pide un rescate económico), no pague el rescate ni siga los pasos indicados en las pantallas de estos virus.
- Si tiene los medios, contrate un profesional especializado a fin de realizar una limpieza del equipo. En algunos casos, ante la imposibilidad de eliminación, el especialista debe respaldar los datos, reinstalar y restaurar.

**Acceso no autorizado y comprobado de Crackers:**

- No abone ningún rescate o acceda a algún chantaje.
- Si está dentro del ámbito de una organización:

  • Comunique inmediatamente la situación a su superior.
  • Cuide la imagen, colaborando en la comunicación adecuada los usuarios internos y externos que usan el/los sistema/s
  • Colabore con los especialistas técnicos a fin de comunicar y publicar opciones alternativas del uso del servicio afectado.

**Estafas y fraudes Informáticos:**

- En el caso de tarjetas de crédito y débito:
  • Comunicarse en forma telefónica con el Banco y/o emisor de la tarjeta a fin de comprobar el hecho y/o denunciar las tarjetas afectadas.
  • Complete el/los formularios si se lo requiere.
  • Documente.
  • Realice, a través de home banking, el stop débito de las operaciones afectadas.
  • Siga los pasos y consejos de su Banco Emisor.

- Si el sitio en el cuál sucedió el incidente lo permite, complete el formulario correspondiente de protección al consumidor o protección de pagos.
- Recopile toda la documentación asociada a los comprobantes de la operación.

# 15. ¿Dónde denunciar y solicitar asesoramiento?

Realice la denuncia correspondiente acompañando toda la evidencia **en la fiscalía más próxima a su domicilio o en la dependencia policial de su jurisdicción.**

## ¿Donde solicitar asesoramiento?

- 911 de la Policía.

- Ministerio Público de Salta (Ciudad Judicial):
  - Teléfono : (0387) 4-258000
  - Mail: contactompf@mpublico.gov.ar
  - Oficina de Orientación y Denuncia: http://www.mpfsalta.gov.ar/OOyD/Oficina-de-Orientacion-y-Denuncia

- Unidad Fiscal Especializada en Ciberdelincuencia :
  - Teléfono : (+5411) 5471-0040
  - Mail: denunciasufeci@mpf.gov.ar

- División Delitos Tecnológicos de la Policía Federal Argentina:
  - Teléfono : (+5411) 4800-1120 / 4370//-5899
  - Mail: delitostecnologicos@policiafederal.gov.ar

- Fiscalía de Primera Instancia N° 1 de Salta:
  - Teléfono: (0387) 4-312313
  - Mail: fisfed1-sta@mpf.gov.ar

## 15.1. Menores

**Línea de atención a Niños, Niñas y Adolescentes**

• Línea 102: Opera en 15 jurisdicciones del país

**Ministerio de Justicia y Derechos Humanos de la Nación**

• Teléfono (sin cargo): 0800-222-1717

• Email: equiponinas@jus.gov.ar

• Web: http://www.jus.gob.ar/atencion-al-ciudadano/atencion-a-las-victimas/brigada-nin@s.aspx

## 15.2. Datos Personales

**Dirección Nacional de Protección de Datos Personales**

• Teléfono : (+5411) 5300-400

• Email: denuncias_pdp@jus.gob.ar

• Web: http://www.jus.gob.ar/datos-personales.aspx

## 15.3. Contenidos de carácter injurioso en Internet

**INADI: Depende del Ministerio de Justicia y Derechos Humanos**

• Teléfono: (+5411)- 4340-9400 / 0800 999 2345

• Teléfono en Salta: (0387) 4-218758

• Email: 0800@inadi.gob.ar

• Email (Salta): salta@inadi.gob.ar

• Web: www.inadi.gob.ar

# 16. Concientización sobre uso responsable de las TIC

Analizados los riesgos existentes en cuanto al uso de la tecnología y la legislación existente en Argentina respecto de los delitos informáticos, se realizó una recopilación de información de diversas fuentes relacionadas con portales y/o organizaciones nacionales e internacionales a fin de promover una serie de recomendaciones con el objeto de concientizar a la sociedad sobre el uso responsable de las TIC y prevenir estos delitos. Las mismas corresponden al concepto de huella digital (identidad, reputación) la navegación segura y responsable de la web, el uso de correos electrónicos, las redes sociales y el cuidado de la privacidad, los teléfonos inteligentes y su uso, etc. En suma, información destinada a adultos, para que puedan ejercer su rol y acompañar a los chicos y las chicas en internet, construyendo diálogo y debatiendo sobre las distintas cuestiones sociales que suceden en estos espacios.

## 16.1. Huella Digital

"Nuestra huella digital está formada por los rastros que dejamos al utilizar Internet:

- Comentarios en redes sociales
- Llamadas de Skype
- El uso de aplicaciones
- Registros de correo electrónico.

Todo esto forma parte de nuestro historial en línea y, potencialmente, puede ser visto por otras personas o almacenado en una base de datos."

Fuente: (https://www.internetsociety.org/es/tu-huella-digital)

En tiempos actuales, Internet es la fuente de información para conocer a una persona. Por ello es primordial el cuidado de lo que se sube, ya que será la vidriera mediante la cual el mundo nos conocerá. Esta recomendación también debe ser entendida por los padres, a fin de orientar a sus hijos, respecto de los contenidos que se publican. Los mismos le pueden jugar en contra en el futuro en cuanto a su reputación y en la búsqueda laboral.

Unicef, mediante su guía de convivencia digital, detalla los siguientes riesgos asociados a la identidad digital:

- Brindar información privada, actual o del pasado, a personas que no tendrían porque recibirla.
- La información privada o íntima publicada en Internet puede tener un sentido en el ámbito privado pero otro muy diferente en el ámbito público.
- La trayectoria o imagen de la persona se vea empañada por información pasada o brindada por terceros. Este tipo de información, ya sea antigua o descontextualizada, quedará asociada a la identidad personal en cada búsqueda que se realice de ese perfil.
- Se puede llegar a adelantar información que comúnmente se brinda cuando se conoce con mayor profundidad a alguien, corriendo el riesgo de adelantar etapas en las relaciones, tanto profesionales como personales.
- El usuario puedo quedar relacionado con actividades o actitudes pasadas o erróneas que afectarán la opinión de quien busque información, pudiendo actuar como filtros de selección que le quiten la oportunidad de presentarse en forma personal.

## 16.2. Equipamiento seguro

Es recomendable:

- Utilizar software legal.
- Descargar todas las actualizaciones disponibles del sistema operativo y/o aplicaciones instaladas.
- Usar antivirus o software de seguridad y procurar que esté siempre actualizado y activado.
- Utilizar contraseñas seguras acceso a los equipos y no la comparta[4].
- Definir patrones y/o contraseñas de acceso seguros en los dispositivos móviles y/o dispositivos de acceso a Internet y no la comparta.
- Instalar, si el dispositivo o sistema operativo lo permite, controles parentales cuando el uso es por parte de menores.
- Tratar de evitar en lo posible el uso de medios removibles desconocidos o de terceros no confiables.
- Realizar backups (copias de seguridad) de la información en forma periódica en dispositivos externos.
- No conectarse a redes Wifi de dudosa procedencia o que no tengan seguridad asociada.
- Si se adquiere un dispositivo usado, asegurarse de borrar en forma segura los datos existentes y reinstalarlo. En igual sentido si está por vender un dispositivo.

*4. Contengan al menos ocho (8) caracteres, incluyan letras y números, no contengan una palabra completa y no tengan relación con información o datos personales del usuario.*

## 16.3. Navegación segura por Internet

Es recomendable:

- Navegar sobre páginas conocidas. Evitar páginas con contenidos nocivos o falsos.
- No usar redes wifi desconocidas y sin seguridad en operaciones sensibles (home banking, acceso a sistemas de una empresa, compras online, viajes online etc.)
- No usar siempre el mismo nombre de usuario y contraseña en todos los servicios que se utilice. Usar contraseñas que contengan por lo menos 8 dígitos y combinar letras y números.
- No proporcione, por principio, datos personales como nombre, dirección, número de DNI, número de teléfono o fotografías suyas o de su familia, profesión y lugar de trabajo. Realizarlo solo en los casos que esté comprobado el sitio que ingresa y sea necesario para realización de un determinado requerimiento comprobado. Verificar además que el sitio tenga registrado su Banco de Datos en algún organismo del estado.
- Evitar aceptar pantallas emergentes de páginas webs con mensajes que indican información falsa como premios, avisos de virus, regalos, promociones, que tratan de que el usuario haga clic sobre ellas para enviarle publicidad o instalarle un programa o malware.
- No hacer click en cualquier enlace o vínculo sospechoso.
- Evitar el ingreso de información personal en formularios dudosos.
- No publicar información privada de otros sin su permiso.
- Tener precaución con los resultados arrojados por buscadores web ya que no siempre indica la información que estamos buscando y además puede indicar una página falsa.
- Descargar aplicaciones desde sitios web oficiales.
- Si se necesita introducir información sensible en un sitio web, asegurarse de que la página es segura (notar que la dirección web comience con "https:", tenga un candado verde o indique sitio "seguro" o "es seguro").
- **No crea todo lo que encuentra, vea o lea en Internet.**
- **Recuerde que todos los datos proporcionados en Internet se almacenan y se distribuyen en distintos servidores y medios de almacenamiento en el lugar geográfico de la Web, en otras Web y/o en distintos países. Por ello la información Internet puede continuar aún online por siempre aunque se la elimine.**

## 16.4. Uso seguro de correos electrónicos

Es recomendable:

- Usar una contraseña segura para su cuenta de correo y no compartirla.
- Verificar la autenticidad del remitente. No abrir mensajes de remitentes desconocidos y que contengan archivos adjuntos.
- No abra mensajes que contengan archivos adjuntos de dudoso nombre y sin solicitarlos.
- No responder a ningún mensaje de correo no solicitado.
- No visitar los sitios Web, ni abrir fotos o links que figuran en los mensajes. Estos links pueden conducir a páginas con algún malware instalado, referenciar a páginas falsas o solicitar información privada.
- No iniciar, contestar ni continuar con las cadenas de mail que por lo general contienen archivos adjuntos y además pasan a pertenecer a listas de direcciones de correo electrónico que son usadas para envío de correo basura(spam) o cualquier otra actitud orientada a confundir el uso al usuario para el robo de datos, estafa o instalación de malware.
- Cuando se realiza un envío masivo, usar las opciones de copia oculta a fin de evitar la propagación de correos electrónicos de otros destinatarios del cual no se tenga el consentimiento.
- No reenviar mensajes privados sin el consentimiento del remitente.

## 16.5. Prevención en las redes sociales

Es recomendable:

- Configurar la privacidad de las redes sociales a fin de controlar que se publica, a quién, cuándo, cómo y los accesos permitidos.
- Tener mucho cuidado en la información que se publica, ya que se torna difícil su eliminación y tener control sobre la misma; ya que puede ser reproducida de manera mal intencionada por otras redes sociales o portales de Internet.
- Evitar agregar o dialogar con personas desconocidas.
- Evitar ingresar a vínculos de desconocidos o reenviados. Tampoco compartirlos ya que puede redireccionar a sitios con malware.
- No proporcionar información sensible como dirección, teléfono, estados, DNI, números de cuentas, fechas de viajes y controlar como se publica y a quien, las fotos y videos privados.
- Evitar realizar comentarios que puedan herir sensibilidades de otras personas.

- No compartir imágenes, vídeos, comentarios o datos personales de contactos sin autorización y que pueda afectar su intimidad.
- No compartir datos o información confidencial de la organización en la que se trabaja. En igual sentido no realizar comentarios que puedan dañar la imagen de dicha organización.

## 16.6. Uso seguro de Smart Phones

Es recomendable:

- Activar el acceso a tu dispositivo mediante contraseña.
- Configurar el bloqueo del dispositivo para que la información no sea vista por extraños.
- Descargar todas las actualizaciones que indique el dispositivo para el sistema operativo.
- Instalar un software de seguridad o software antivirus.
- Descargar aplicaciones sólo desde tiendas oficiales. Revisar los permisos de las mismas. Es muy aconsejable leerlos y, de no estar seguro de lo que implican, evitar instalar la aplicación.
- No activar conexiones por bluetooth, infrarrojo, Wi-Fi y Geolocalización por defecto.
- Desactivar la ubicación GPS para las fotografías. Si las mismas son subidas a una red social o algún portal, puede indicar las coordenadas exactas de una ubicación. Esto puede ser aprovechado por ciberdelicuentes para determinar si una persona está en su domicilio.
- No ingresar en el dispositivo tarjetas de memoria sin haber comprobado que estén libres de virus/malware.
- No acceder a enlaces facilitados a través de mensajes SMS/MMS no solicitados y que impliquen la descarga de contenidos en el equipo.
- Agendar el número IMEI de tu teléfono, ya que es único para cada dispositivo en todo el mundo y permite desactivar el teléfono en caso de robo.
- Si posee información confidencial o sensible, activar las opciones de cifrado de la tarjeta o dispositivo.
- Si existe la opción, puede activar aplicaciones de Administración remota a fin de localizar y borrar datos en situaciones de robo o pérdida del dispositivo.
- Realizar copias de seguridad de los datos del dispositivo frecuentemente.
- Realizar un borrado seguro de los datos antes de venderlo o darle de baja.

## 16.7. Rol de la familia – Padres y menores

Es recomendable:

- Utilizar y aplicar todas las recomendaciones mencionadas anteriormente respecto al equipamiento, navegación, correo electrónico, redes sociales y SmartPhones.
- Establecer reglas claras para el uso de internet en la familia.
- Instalar aplicaciones de control parental.
- Administrar las descargas de juegos y aplicaciones apropiados para cada edad del menor.
- Orientar, acompañar y/o asistir en el uso e ingreso en los distintos servicios de Internet (navegación, usuarios, claves, correo, foros, redes sociales, plataformas educativas, etc. Tener una actitud activa y presencial.
- Observar y detectar actitudes o conductas nuevas que pueden inducir situaciones relacionadas con el uso de la red.
- Participar en la comunidad educativa escuchando, opinando, recomendando y/o realizando acciones tendientes a capacitarse y entrenarse sobre el uso de la tecnología y sus riesgos asociados.

- Educar a los menores sobre:
  - El uso de Internet y los riesgos asociados a su mal uso.
  - La importancia de lo que se publica, se comparte, se comenta y la confidencialidad de la información personal. Lo que se cargue en la red puede quedar relacionado con actividades o actitudes pasadas o erróneas que afectarán la opinión de quien busque información, pudiendo actuar como filtros de selección que le quiten la oportunidad de presentarse en forma personal y laboral en el futuro.
  - Lo que debería ser público y privado. Proteger la privacidad e intimidad.
  - La necesidad de no hablar con extraños en redes sociales y chats.
  - El reporte inmediato a la familia sobre situaciones extrañas que encuentren en la red.

# 17. Referencias y fuentes consultadas


- Guía de sensibilización sobre Convivencia Digital (Unicef, Gobierno de la provincia de Bs. As. y Faro Digital).
- Sistema Argentino de Información Jurídica - Delitos Informáticos (Identificación SAIJ : A0077928).
- El rastro Digital del Delito (Universidad Fasta – Autores Di Iorio, Constanzo, Curti y otros).
- Argentina Cibersegura – Groomming.
- Argentina Cibersegura – Guía Bulling.
- Argentina Cibersegura – Guía Familia.
- Argentina Cibersegura – Guía Mayores.
- Argentina Cibersegura – Guía navegación menores.
- Argentina Cibersegura – Guía navegación.
- Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado 1ra. Parte. (Temperini, Marcelo).
- Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado 2da. Parte. (Temperini, Marcelo).
- Una aproximación a la estadística criminal sobre delitos informáticos (SAIJ – Ministerio de Justicia y Derechos Humanos de la Nación).
- Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 (Del Pino, Santiago).
- Eset –Guía del empleado seguro.
- Eset –Guía de seguridad en Android.
- Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Naciones Unidas).
- Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC) - Manejo de Incidentes.
- Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC) – Guía práctica para denunciar un delito informático.
- Código Penal Argentino.
- Código Civil y Comercial Argentino.

## 17.1. Otras referencias de sitios Web:

- http://www.symantec.com/region/mx/avcenter/cybercrime/pharming.html
- https://www.bbva.com/es/skimming-la-estafa-la-clonacion-tarjetas/
- http://blog.segu-info.com.ar/2010/06/proyecto-de-ley-robo-de-identidad.html
- http://www.senado.gov.ar/parlamentario/parlamentaria/309486/downloadPdf
- http://43jaiio.sadio.org.ar/proceedings/SID/13.pdf
- http://www.lanacion.com.ar/1972743-delitos-informaticos-cuando-la-tecnologia-y-las-redes-van-mas-rapido-que-la-legislacion
- https://issuu.com/elderechoinformatico.com/docs/revista_22
- http://www.migliorisiabogados.com/los-ciberejercitos-civiles-y-regulares/
- http://www.informaticalegal.com.ar/2001/11/23/convencion-de-budapest-sobre-ciberdelincuencia/
- https://computing799.wordpress.com/como-proceder-ante-un-virus-informatico/
- http://soporte.eset-la.com/kb2505/?page=content&id=SOLN2505&querysource=external_es&locale=es_ES
- http://soporte.eset-la.com/kb2563/?page=content&id=SOLN2563&querysource=external_es&locale=es_ES
- https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201212_sp.pdf
- http://www.buenosaires.gob.ar/noticias/consejos-de-uso-seguro-de-internet-y-redes-sociales

## 17.2. Glosario: El ABC de la Web (Faro Digital)

A modo complementario con la información detallada en esta guía puede consultar de manera on line un glosario realizado por Faro Digital donde encontrará una lista con las definiciones de los términos más usados en la cultura digital. Se accede a través de la siguiente página web:

- http://www.farodigital.org/portfolio/el-abc-de-las-redes/

# 18. ANEXO - El ABC de la web (Faro Digital)

**Antivirus**
Programas dedicados a la detección y remoción de virus. Los mismos pueden ser utilizados en una computadora convencional como así también ensmartphones, tabletas u otros dispositivos electrónicos con conexión a Internet. En algunos casos, los antivirus más desarrollados del mercado se complementan con servicios de firewall, anti-malware y anti-spyware.

**App**
Una App, o simplemente "aplicación", es un software que se instala en unsmartphone o tableta. Tienen como objeto maximizar el uso de los dispositivos electrónicos ya que le agregan al mismo alguna prestación. Existen apps de distintas categorías como: Educación, Deportes, Noticias, Entretenimiento, Salud, Juegos, Fotografía, Tiempo, etc. En los teléfonos inteligentes tabletas vendrían a reemplazar a los "Programas" de las PC de escritorio. El significado de "App" proviene de la palabra del inglés "application" que en español significa "aplicación".

**Big Data**
El concepto Big Data remite a la arquitectura de grandes volúmenes de datos. Es el tratamiento y análisis de grandes volúmenes de información incrementado, entre otras causas, por el avance de la interconexión global.

**Bluetooth (BT)**
Es una tecnología de transmisión de datos de corto alcance entre dispositivos electrónicos (smartphones, tabletas, notebooks, etc.). Si bien varía según las circunstancias espaciales, el promedio de distancia de transferencia ronda los 10 metros. En sus inicios el único fin era el de intercambiar archivos, en la actualidad sus funciones comenzaron a maximizarse, llegando a auriculares, parlantes, stereos y monopods.

**Bot**
Un bot es un programa de origen malicioso que posee como objetivo que un tercero tome el control de un dispositivo infectado de manera remota.

**Botnet**
Es una red de computadoras infectadas por un bot, es decir, por un software malicioso que permite el control remoto por parte de un tercero.

**Byte**
Es una unidad de medición de almacenamiento utilizado en informática y telecomunicaciones. Un Byte equivale a 8 bits.

**Ciberbullying**
También conocido como ciberacoso, es el proceso por el cual un niño, niña o adolescente es atormentado, acosado, amenazado, humillado y avergonzado por parte de un par a través de Internet.

**Cloud computing**
La traducción al castellano sería "computación en la nube" o "la nube" simplemente. Es un servicio que se brinda a través de una red permitiendo principalmente el almacenamiento de información.

**Código QR**
El "Quick Response Code" o "código de respuesta rápida" es un patrón ilegible para el ojo humano, descifrable a través de un lector especial. El mismo almacena información alfanumérica con un máximo de 4.200 caracteres. Se encuentra compuesto por tres cuadrados de gran dimensión distribuidos en sus vértices izquierdos y superior derecho que determinan el sentido de su lectura y pequeños cuadrados en su interior. Su antecesor es el "Código de Barras Bidimensional".

**Control parental**
El control parental es una función orientada al público adulto que posee como objetivo fundamental bloquear o limitar el acceso de l@s chic@s a sitios que no son aptos para ellos, ya sea por su contenido sexual o violento, o por los riesgos que pueden correr. Esta función la encontramos en diferentes antivirus como así también en algunos sistemas operativos o aplicaciones que pueden descargarse de la Web.

**Cyberdating**
El cyberdating o "cita virtual" que también es conocido como "online dating" remite a la acción de conocer personas por Internet para concretar citas presenciales. Es la "cita a ciegas" del siglo XXI en donde se utilizan las ventajas de la red para conectarse con personas que poseen intereses similares a los nuestros. Si bien esto ya podía realizarse a través de sitios de chats o redes sociales, en la actualidad se encuentra en crecimiento el uso de aplicaciones específicas para este fin como ser Tinder, Adoptauntio, Meetic, eDarling, entre otras.

**Datos personales**
Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. Desde el año 2000 en Argentina existe la Ley 25.326 que protege los mismos.

**Datos sensibles**
Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Desde el año 2000 en Argentina existe la Ley 25.326 que protege los mismos y en su Artículo 7 afirma que ninguna persona está obligada a proporcionarlos.

**Delito informático**
También conocido como "ciberdelito" remite a cualquier actividad ilegal convencional (robo, hurto, fraude, estafa, falsificación, etc.) que utilice como medio a la informática. Desde el año 2008 en Argentina existe la Ley 26.388 que incorpora al Código Penal esta tipificación delictiva.

**Emoji**
Un emoji es la versión japonesa de los emoticones occidentales. Son dibujos predeterminados utilizados en las aplicaciones de chat que representan situaciones o estados de ánimo.

**Emoticón**
La palabra "emoticón" proviene de la suma de los términos "emoción" e "ícono" y remite a una secuencia de caracteres que expresan un estado de ánimo por medio de la invención gráfica de una cara. Los más populares son ":)" o ":(" que representan sonrisa y tristeza respectivamente.

**FAQ**
Del inglés Frequently Asked Questions son las populares "preguntas frecuentes" que encontramos en muchos sitios web o aplicaciones populares. Las mismas poseen el fin de evitar el tráfico innecesario de mensajes y correos electrónicos con inquietudes ya resultas. Las FAQ son una gran herramienta para ayudar a los nuevos usuarios a dar los primeros pasos sin necesidad de realizar consultas básicas a los webmasters o administradores de los sites.

**Flirtmoji**
Son emoticones con connotación sexual explícita o implícita. Los mismos se encuentran disponibles en diferentes aplicaciones de mensajería instantánea.

**Geek**
Es la personas apasionada y amante de la tecnología, pero que además posee un amplio conocimiento sobre la temática mencionada.

**Geolocalización**
La geolocalización o georreferenciación es la posibilidad de conocer la ubicación puntual de un objeto. Son cada vez más los dispositivos electrónicos que poseen GPS integrado, lo que incrementa las posibilidades de situar geográficamente la información publicada. Con mayor frecuencia comienzan a observarse en las redes sociales posteos georreferenciados o aplicaciones que permiten almacenar coordenadas espaciales.
Al mismo tiempo, el auge de Internet de las Cosas también se involucra con la geolocalización a fin de maximizar las prestaciones convencionales de los objetos, sujetos y hasta animales, tal cual observamos en los siguientes ejemplos:

**• Cámaras fotográficas que registran el lugar exacto en donde tomaron una imagen.**

**• Aplicaciones que permiten conocer todas las coordenadas en donde nuestro vehículo se encuentra estacionado.**
**• Dispositivos que permitan observar dónde se encuentra nuestra mascota.**
**• Publicaciones en redes sociales que muestren el sitio en donde fueron posteados.**

## Guest posting

También conocido como "Guest Blogging" (en español "publicación de huésped o invitado") es una táctica de cooperación entre bloggers. La acción se inicia cuando un blogger invita a otro a que participe mediante la redacción de una publicación. El objetivo final es que el invitado se dé a conocer en el nicho temático que trata el sitio con el fin de captar nuevos seguidores. Asimismo, a través de guest posting el anfitrión busca incrementar la calidad de su blog.

## Hacker

Es aquella persona especialista en alguna rama de la tecnología que es capaz de realizar intervenciones en redes, penetrando en bases de datos o sistemas informáticos que no son de acceso público. Si bien el término posee habitualmente una connotación negativa ya que se la emparenta con la figura de un pirata o un intruso, el hacker, al ser un especialista, trabaja también para desarrollar redes y sistemas más seguros.

## Hardware

El hardware remite a las partes físicas de una computadora, es decir, lo que se puede ver y tocar. La palabra surge de la unión de dos términos de la lengua inglesa: hard (duro) y ware (utensilio).

## Hashtag

Proveniente del idioma inglés, un hashtag ("etiqueta" en español) es un término que se popularizó con la masificación de las redes sociales y que refiere a un conjunto de caracteres antepuestos por el símbolo "#" que sirve para ordenar los mensajes en base a una temática determinada. Si bien se lo relaciona con Twitter, su uso es también propio de diferentes redes sociales como Facebook o Instagram.

## Hoax

Es un término del idioma inglés que significa "farsa" o "fraude". Remite a un mensaje falso distribuido por correo electrónico o a través de la construcción de una página web con el único objetivo de brindar información carente de veracidad. En algunas ocasiones se utiliza para captar direcciones de correo electrónico para futuros spams, en otras, para revelar contraseñas.

## Identidad digital

También conocida como Identidad 2.0, es la recopilación de información que un usuario construye en Internet a través de la información que publica al interactuar con otras personas en sitios webs y redes sociales.

**Inmigrante digital**
A diferencia del nativo digital, el inmigrante es la persona mayor de 35 años que no se ha criado desde su nacimiento en un mundo de dispositivos tecnológicos interconectados y que debe inmiscuirse en dichas temáticas para poder interactuar con plenitud en él.

**Internet de las cosas**
El Internet de las Cosas (IoT en inglés) es un concepto que postula la conexión a la red de ciertos objetos que hasta hace un tiempo se pensaban inertes o aislados de la vida interconectada. Es decir, pensar objetos cotidianos conectados a la red. Ej: Una heladera que avise la fecha de vencimiento de los alimentos; un aire acondicionado que pueda controlarse desde un teléfono celular; un lavarropas que nos envíe un mensaje de texto al finalizar un lavado. Estas son algunas de las cosas que en un futuro cercano podrían ser parte de la red y otorgarle al usuario nuevas funciones a la fecha impensadas.

**Keylogger**
Los keyloggers son un tipo de software que almacena todo lo registrado a través de un teclado de computadora. Es un término derivado del idioma inglés (key = tecla y logger = registro) que tiene como objeto que un tercero malintencionado puede conocer todos los movimientos y la información que el usuario portador del malware registre en su ordenador personal.

**Link building**
Es una técnica de marketing online que busca posicionar de mejor manera nuestra página web. La tarea suele ser desarrollada por un linkbuilder o especialista en SEO (search engine optimization) quien conoce las técnicas para optimizar los motores de búsqueda y obtener mejores resultados, por ende, un mejor posicionamiento web.

**LOL**
LOL es una sigla que se popularizó en Internet. La misma deriva del idioma inglés y significa “Laughing Out Loud”, “Laugh Out Lots” o “Lots OfLaughs”, en español “riendo a carcajadas” o “reír en voz alta”. Habitualmente es utilizada para comentar en redes sociales o en chats reemplazando al tradicional “jajaja”. En ocasiones puede ser reemplazado por “XD”, que es un emoticón en forma de texto que representa a una cara riendo a carcajadas.

**Meme**
Si bien no existen definiciones exactas de lo que son los memes, estos responden a ideas, conceptos y expresiones que se viralizan de una manera sorprendentemente veloz, teniendo la capacidad de reproducirse de manera exponencial. Los memes son una suerte de “moda de Internet” que pueden ser expresados en diferentes formatos (imágenes, texto, audio o video) con el objetivo de ser difundidos por las redes sociales o los sistemas de chats, siempre y cuando cuenten con características claves: ser interesantes, provocadores y originales.

Asimismo, para ser considerado un meme es imprescindible poseer un ciclo de vida muy corto ya que nacen, se reproducen y caen en el olvido en un segmento temporal muy pequeño. Tal es el nivel de popularidad que han logrado los memes, que en la actualidad no son indispensables los conocimientos de retoque digital o edición de audio y video, sino que existen sites dedicados exclusivamente a la personalización de estos.

**Microblogging**
El microblogging es un servicio para enviar y recibir mensajes breves, con caracteres limitados. Los dos ejemplos más populares son los mensajes de texto SMS y los Tweets que permiten 140 caracteres alfanuméricos.

**Nativo digital**
El nativo digital es la persona que se ha criado en un mundo en donde lasTecnologías de Información y Comunicación (TIC) han comenzado a ocupar cada vez más espacios de la vida cotidiana. Al ser contemporáneos a esta transformación el proceso de aprendizaje que necesitan para el uso de estas TICes casi nulo respecto de las personas denominadas inmigrantes digitales que necesitan comprender y aprender el uso de los nuevos dispositivos electrónicos.

**Nomofobia**
La nomofobia (proviene de la frase en inglés “no mobile phone phobia”) es el miedo irracional a no poseer nuestro teléfono móvil. Es la angustia que se presenta al olvidarnos el smartphone o quedarnos sin batería y sentirnos desconectados del mundo. Si bien habitualmente se relaciona la nomofobia a los teléfonos celulares, el concepto engloba a todo tipo de dispositivos electrónicos que nos permiten conectarnos a Internet como también a una tableta o PC.

**Password**
En español “clave” o “contraseña” es un conjunto de caracteres alfanuméricos que nos permite el ingreso a un determinado sitio web o aplicación. El correcto uso de un password incrementa nuestra privacidad y seguridad a la hora de resguardar nuestra información personal.

**Phishing**
Es uno de los métodos más utilizados por los delincuentes informáticos. Posee como objetivo principal captar información confidencial como ser nombres de usuarios, contraseñas, números de cuentas bancarias, etc. Una de las formas más utilizadas para llevar a cabo el phishing es a través del correo electrónico o de una página web falsa que imita a un sitio verdadero y solicita información personal para engañar al usuario.

**Phubbing**
Phubbing es un término que se forma al unir las palabras en inglés phone(teléfono) y snubbing (despreciar/menospreciar) que surge en el marco del auge de los smartphones. Se define phubbing a la situación en la

cual una persona (el phubber) presta más atención a un teléfono o dispositivo electrónico que a la situación social que posee a su alrededor.

**Pic**
Pic es la abreviatura de la palabra de origen inglés picture que en español significa "imagen", siendo un término que se popularizó entre usuarios de redes sociales.

**QWERTY**
El QWERTY es un estilo de teclado que refiere a la distribución de las teclas. Según especialistas, data de las primeras máquinas de escribir mecánicas y el orden de las letras busca que las dos manos sean utilizadas de igual forma para escribir la mayoría de las palabras.

**Realidad Aumentada**
Consiste en combinar el mundo real con el virtual mediante un proceso informático. El resultado es una visión a través de un dispositivo tecnológico de un entorno físico real, cuyos elementos se combinan con elementos virtuales para la creación de una realidad mixta en tiempo real. O sea, se añade información virtual a la información física ya existente. La principal diferencia con la realidad virtual es que no reemplaza la realidad física, sino que agrega datos informáticos al mundo real. Creando así distintos tipos de experiencias interactivas para el usuario, por ejemplo: catálogos de productos en 3D, probadores de ropa virtual, videojuegos, etc.

**Reputación Web**
La reputación web es la imagen, el prestigio y la referencia que Internet muestra de una persona. Si bien el concepto se encuentra vinculado a la Identidad Digital, la reputación web no solo es construida por el propio usuario sino que también poseen un papel preponderante las omisiones y las acciones de terceros.

**Retweet**
Es el reenvío de un tweet, es decir de una publicación de otro usuario. Consiste en replicar esa información para que todos los seguidores de nuestro perfil puedan acceder a la misma. Es una acción que se realiza fácilmente y sirve para difundir y viralizar la información.

**Seguridad informática**
La seguridad informática es el conjunto de acciones que se llevan a cabo para lograr que un sistema sea la más seguro posible. Es decir, es un conglomerado de herramientas que se utiliza para lograr la inviolabilidad de la información o los datos de un sistema informático.

**Smartphone**
También conocido como "teléfono inteligente" según su traducción del inglés, es un disposito móvil capaz de efectuar una gran cantidad de tareas que los teléfonos celulares convencionales se veían impedidos de realizar.

En la actualidad existe un debate para determinar si un smartphone es un teléfono móvil al cual se le pueden añadir funciones o si es una computadora en miniatura que entre otras cosas puede ser utilizado como teléfono.

## Stalkear

Es un término que deriva del inglés ("to stalk") que equivale a acosar, espiar o perseguir. Por lo general se utiliza para denominar a la acción que se da en entornos tecnológicos, y en especial redes sociales. Por lo que sería la acción de acechar o acosar de manera digital (online) observando el perfil de un usuario (sus fotos, comentarios, videos, etc.) a través de Facebook, Twitter, Instagram, Tumblr, Google +, y otras redes. La persona que lo ejerce recibe la denominación de "Stalker". Y la acción puede ser llamada "Stalkear", por ejemplo: Juan estástalkeando a María.

## #TBT

#TBT es un hashtag de Instagram que significa "Throwback Thursday", en español "jueves de antaño", creado por los mismos usuarios de la red social con la finalidad de postear una fotografía de su infancia únicamente ese día de la semana.

## TIC

El término TIC es una sigla que significa "Tecnologías de Información y Comunicación" y refiere a todos los recursos y herramientas que procesan, almacenan, envían y reciben información de un sitio a otro, mediante un soporte tecnológico.

## Trending Topic

También conocido como "TT", significa "tendencia" y es utilizado en Twitter para identificar los hashtag más populares del momento, es decir, son los temas más hablados en la red social.

## Tweet

Es la expresión en la red social Twitter de un mensaje, pensamiento, idea, frase, momento, publicación, etc. El mismo puede tener como máximo 140 caracteres. En esta red social encontraremos tweets de todos los usuarios que deseamos seguir, y nos aparecerán enlistados en nuestra página de inicio. A través de lostweets nos podremos enterar las notificaciones de las personas que nos interesan, sean amigos, famosos, periodistas, artistas u otros.

## URL

El Uniform Resource Locator proviene del idioma inglés y significa "localizador uniforme de recursos". Es la ruta o dirección de un sitio web que es colocada en la barra de navegación para que nos dirija a un lugar determinado. Se encuentra compuesta por tres partes: protocolo, dominio y ruta. Ejemplo: http://www.convosenlaweb.gob.ar/adolescentes/glosario.aspx

- Protocolo: "http://".
- Dominio: "www.convosenlaweb.gob.ar".
- Ruta: "/adolescentes/glosario.aspx".

**Web Cam**
Es una cámara digital que filma imágenes y que suele colocarse en la parte superior del dispositivo tecnológico (PC, note/netbook). Estas imágenes pueden ser transmitidas de manera directa a través de Internet, ya sea a una página web, sala de chat, red social, o bien a otro dispositivo tecnológico o Pc de forma privada. Estas cámaras son frecuentemente utilizadas por chicos y chicas para comunicarse con sus pares en sitios de mensajería instantánea o chat comoSkype, Line, Hangouts, Chatroulette, Omegle, etc.

**WiFi**
El WiFi, también conocido como “wifi” o “wi-fi”, es un método de conexión inalámbrica derivado de una marca comercial (Wireless Ethernet Compatibility Alliance, conocida como Wi-Fi Alliance) que con el tiempo se ha popularizado hasta convertirse en nombre propio. Esta tecnología permite conectar computadoras, televisores, impresoras, consolas de videojuegos, smartphones, tabletas, entre una gran gama de dispositivos electrónicos que se van incrementando con el tiempo. Si bien la capacidad de conexión es limitada espacialmente, según la potencia del enrutador se puede maximizar el alcance de la señal.

**Wiki**
Se denomina de esta manera a las páginas web colaborativas, en donde los usuarios pueden editar directamente desde el navegador. Así se pueden crear, modificar o bien eliminar contenidos, que luego son compartidos. Es un sistema de trabajo que brindan sitios web para crear contenido e información de manera sencilla. El sitio web ejemplificador por excelencia es Wikipedia, la mayor enciclopedia digital de contenidos web.

**WTF**
WTF es otra de las abreviaturas que se popularizaron en Internet usadas a la hora de comentar en las redes sociales o en los sitios de chats. La misma es una sigla proveniente del idioma inglés que significa “What the fuck”, en español “¡qué demonios!”, utilizada en la red para comentar situaciones que nos parecen increíbles o nos dejan con la boca abierta.

# 19. Material Audiovisual sugerido

## Qué son los delitos informáticos o ciberdelitos

1. **Unidad Fiscal Especializada en Ciberdelincuencia (UFECI | Ministerio Público Fiscal | Procuración General de la Nación)**

   Video de concientización. Narra la historia de una joven que sufrió el robo de las contraseñas para acceder a sus casillas de correo electrónico y sus redes sociales.
   **Link**:
   https://www.youtube.com/watch?v=ru2PH4Z2xMc&t=63s

## Menores

1. **Unidad Fiscal Especializada en Ciberdelincuencia (UFECI | Ministerio Público Fiscal | Procuración General de la Nación)**

   Videos relacionados a la prevención en redes sociales y chat, como compartir las fotos, protección de las claves y tips de seguridad para no ser víctima en las redes sociales.
   **Link**:
   https://www.mpf.gob.ar/ufeci/enlaces/recursos/

2. **Programa Nacional con vos en la Web (dependiente de la Dirección Nacional de Protección de Datos personales de Argentina)**

   a) Vídeos relacionados con la discriminación en la web, riesgo de hablar con desconocidos, ciberbullying y padres en la Web.
   **Link:**
   http://www.convosenlaweb.gob.ar/materiales/videos.aspx

   b) Guías de actividades de Gromming y Ciberbulling con links a videos relacionados dirigido a niños entre 11 a 18 años.
   **Links:**
   http://www.convosenlaweb.gob.ar/media/2831558/actividades_grooming.pdf

   http://www.convosenlaweb.gob.ar/media/2838679/actividades_ciberbullying.pdf

   http://www.convosenlaweb.gob.ar/media/2915019/guia_actividades_ciberbullying02.pdf

c) Actividades para los niños y adolescentes a realizarse en las aulas de escuelas (sopas de letras, cuestionarios, juegos, etc) de los temas de protección de datos personales y la privacidad.
**Link:**
http://www.convosenlaweb.gob.ar/actividades-para-el-aula.aspx

3. **"Pantallas Amigas" (Organización Española que cuenta con el apoyo de EDEX, organización no lucrativa de acción social con más de 30 años de trayectoria en el impulso del desarrollo integral de la infancia y la adolescencia. Recibe el asesoramiento técnico de Integral de Medios, consultora especializada en educación y nuevas tecnologías desde 1996)**

   a) Recursos educativos y material didáctico orientado a jóvenes y adolescentes.
   **Link:**
   http://www.pantallasamigas.net/

   b) Videos educativos orientados a jóvenes y adolescentes.
   **Link:**
   https://www.youtube.com/user/pantallasamigas

4. **Argentina Cibersegura (Asociación Civil especializada en la concientización y educación sobre el uso seguro de Internet y de las tecnologías de la comunicación**

   Juegos y actividades orientados a niños y jóvenes para concientizar sobre los riesgos en Internet.
   **Link**
   https://www.argentinacibersegura.org/admin/resources/files/consejos/45/AC_Libro-de-juegos-Sponsor_DIGITAL.pdf

## Datos personales

1. **Documentales Televisión Española**

   a) Ojo con tus datos. Documental que aborda la privacidad y el tratamiento de datos personales en la red.
   **Link:**
   http://www.rtve.es/alacarta/videos/documentos-tv/documentos-tv-ojo-tus-datos/2270048/

b) “Big Data, conviviendo con el algoritmo”: Documental relacionado con algoritmos que predicen nuestro comportamiento y nos acerca a un mundo de decisiones tomadas por la inteligencia artificial.
**Link:**
http://www.rtve.es/alacarta/videos/documentos-tv/documentos-tv-big-data-conviviendo-algoritmo/3893978/

2. **Programa Nacional con vos en la Web (dependiente de la Dirección Nacional de Protección de Datos personales de Argentina)**

   Actividades para los niños y adolescentes a realizarse en las aulas de escuelas (sopas de letras, cuestionarios, juegos, etc) de los temas de protección de datos personales y la privacidad.
   **Link:**
   http://www.convosenlaweb.gob.ar/actividades-para-el-aula.aspx

## Daño Informático

1. **Panda Security (Empresa de antivirus)**

   a) Video “Tipo de virus”
   **Link:**
   https://www.youtube.com/watch?v=xWzhpHg9MuE

   b) Video “¿Que es un Ransomware?”
   **Link:**
   https://www.youtube.com/watch?v=2XY9nkiWGW8

2. **“Pantallas Amigas” (Organización Española que cuenta con el apoyo de EDEX, organización no lucrativa de acción social con más de 30 años de trayectoria en el impulso del desarrollo integral de la infancia y la adolescencia. Recibe el asesoramiento técnico de Integral de Medios , consultora especializada en educación y nuevas tecnologías desde 1996)**

   Videos animados relacionados con los virus informáticos y sus tipos.
   **Links:**
   https://www.youtube.com/watch?v=2cZ73Tx2cK4

   https://www.youtube.com/watch?v=4TCS1rQKOnM

   https://www.youtube.com/watch?v=7rxXeojyXXM

3. **Trend Micro (empresa de antivirus)**

   Blog de seguridad, informes, estadísticas y análisis de virus informáticos.
   **Link:**
   http://blog.trendmicro.es/?cat=25

## Acceso indebido, interceptación e interrupción de comunicaciones electrónicas y telecomunicaciones. Publicación indebida

1. **Revista de tecnología "Computer Hoy"**

   Informe año 2017 respecto a millones de cuentas de correo robadas en el mundo.
   **Link:**
   http://computerhoy.com/noticias/internet/filtran-millones-contrasenas-internet-esta-tuya-peligro-62382

2. **Ayuda sobre cuentas robadas de las principales redes sociales y empresas proveedoras de cuentas de correo.**

   **Links:**
   https://es-la.facebook.com/help/131719720300233

   https://support.twitter.com/forms/hacked

   https://help.instagram.com/1068717813216421

   https://es-us.ayuda.yahoo.com/kb/account/Problemas-para-iniciar-sesi%C3%B3n-en-tu-cuenta-de-Yahoo-sln2051.html

   https://account.live.com/acsr?mkt=es-MX

   https://support.google.com/accounts/answer/6294825?hl=es-419

3. **Ted x Madrid año 2015 (Conferencia anual de Tecnología, Entretenimiento y Diseño)**

   Conferencia "¿Por qué me vigilan, si no soy nadie?", realizada por Marta Peirano (periodista reconocida a nivel mundial que escribe sobre tecnología, Entretenimiento y Diseño)

**Link:**
https://www.youtube.com/watch?v=NPE7i8wuupk

## Acceso indebido a un sistema o dato informático

1. **Youtube - Sitio de videos**

   Video subido respecto a un documental emitido por el canal Discovery Chanel, sobre la historia de los Hackers Informáticos.
   **Link:**
   https://www.youtube.com/watch?v=AZCwMVgYGMI

2. **Revista de tecnología "Computer Hoy"**

   Video donde describe los distintos tipos de hackers.
   **Link:**
   https://www.youtube.com/watch?v=qxa8zvRdpC4

## Propiedad Intelectual Software

1. **Diario digital argentino IProfesional**

   Informe del BSA, una alianza mundial de fabricantes de programas informáticos, sobre los riegos del uso de software pirata

   **Link:**
   http://www.iprofesional.com/notas/208703-El-software-pirata-una-puerta-abierta-para-los-delincuentes-informaticos-en-las-empresas

2. **Diario digital argentino Cronista**

   Informe del BSA, una alianza mundial de fabricantes de programas informáticos, sobre estadísticas de Argentina en el uso de software pirata
   **Link:**
   https://www.cronista.com/itbusiness/La-Argentina-el-mas-pirata-de-la-region-casi-70-del-software-es-ilegal-20160531-0009.html

3. **Youtube - Sitio de videos**

   Video (en inglés) Introductorio de Microsoft sobre la serie animada "Genuine Fact Files Archivos de hechos genuinos)" que plantea los riesgos que conlleva la descarga ilegal de software de la Web

**Link:**
https://www.youtube.com/watch?v=NyGmHdHXvS0

## Fraude y estafa informática

**1. Youtube - Sitio de videos**

a) Uso del skimming en Argentina
Link:
https://www.youtube.com/watch?v=lSXWVAuOSIA

b) Recomendaciones del Ministerio del Interior de Perú sobre " ¿Cómo evitar ser víctima de un fraude informático?"
**Link**:
https://www.youtube.com/watch?v=k5M4n5Xcsb0

c) Recomendaciones de la Oficina de Información al Consumidor, OMIC (BS. As. ) respecto a "Cómo evitar las estafas informáticas"
**Link:**
https://www.youtube.com/watch?v=__07VSwKtU4

d) Informe del periodista Klipphan, del medio C5N respecto a las "Estafas Informáticas"
**Link:**
https://www.youtube.com/watch?v=Ja0oDFPhNTI

**2. Recomendaciones de seguridad de los principales Bancos de Argentina**

a) Banco Macro:
https://www.macro.com.ar/PortalMacro/faces/pages_canales/personas/macronline/medidas_de_seguridad?

b) Banco Nación:
https://www.bna.com.ar/Personas/TarjetasDeCredito/ProtejaSusDatos

c) Banco Hipotecario:
https://www.hipotecario.com.ar/default.asp?id=249

d) Banco Mas Ventas:
https://www.bancomasventas.com.ar/informacion-util/recomendaciones-de-seguridad/

e) Banco Santander Rio:
http://www.santanderrio.com.ar/exec/micrositios/opere_seguro/emailsysms.html

f) Banco Galicia:
http://www.bancogalicia.com/banca/online/web/Personas/ProductosyServicios/QueNecesitaSaber/Phishing/

g) Banco Francés:
https://www.bbvafrances.com.ar/meta/francesnet/login/proteja-pc/

h) Banco Itaú:
http://www.itau.com.ar/seguridad/Paginas/fraudes.aspx

## Concientización sobre el uso responsable de las Tics

1. **"Pantallas Amigas" (Organización Española que cuenta con el apoyo de EDEX, organización no lucrativa de acción social con más de 30 años de trayectoria en el impulso del desarrollo integral de la infancia y la adolescencia. Recibe el asesoramiento técnico de Integral de Medios , consultora especializada en educación y nuevas tecnologías desde 1996)**

   a) Recursos educativos y material didáctico orientado a jóvenes y adolescentes.
   **Link:**
   http://www.pantallasamigas.net/

   b) Videos educativos orientados a jóvenes y adolescentes.
   **Link:**
   https://www.youtube.com/user/pantallasamigas

2. **"Guía Infantil" (Revista argentina en Internet que trata de temas de educación y salud de los niños)**

   Recursos educativos y material didáctico sobre nuevas tecnologías.
   **Link:**
   https://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/como-y-cuando-introducir-las-nuevas-tecnologias-en-la-vida-de-un-nino/

**3. Youtube - Sitio de videos**

a) Canal Aula Planeta (Organización española que Impulsa proyectos y soluciones educativas digitales de carácter innovador para la evolución y mejora del aprendizaje del alumno)

Video: Protección ante el uso de las TIC - Campaña de concienciación
**Link**:
https://www.youtube.com/watch?v=Tod4lcakFw4

b) Eset Latinoamerica (Empresa de antivirus internacional)
Video: Internet Sano

**Link:**
https://www.youtube.com/watch?v=0wevcdQ-xc0

c)Ministerio TIC de Colombia

Video: Claves para el uso adecuado de las tic e internet
**Link:**
https://www.youtube.com/watch?v=GW1j2I6EcU8

d) Internet Society (Organización mundial que estudia el comportamiento en Internet) Video: Cuatro Razones Para Cuidar Nuestras Huellas Digitales

**Link:**
https://www.youtube.com/watch?v=cpH-zSRV6Ug

e) CyLDigital (Espacio digital orientado a las Tecnologías de Información)

Video: La huella digital en Internet: reputación online
**Link:**
https://www.youtube.com/watch?v=pZrMxQnY0lU

f) Campus Virtual de Educacón Digital (Espacio digital de formación y acompañamiento pedagógico tendiente a integrar la cultura digital en las escuelas de la Ciudad Autónoma de Buenos Aires orientado a las Tecnologías de Información)

Video: Huella Digital: construir una identidad digital

**Link:**
https://www.youtube.com/watch?v=fLKPsy2_2Og

g) Editorial Santillana

Video: El rol de los padres en la Era Digital
**Link:**
https://www.youtube.com/watch?v=tzwk05qYcI4

h) Tren Digital (organismo dependiente de la Facultad de Comunicaciones de la Universidad Católica de Chile)

Video: El Rol de las TICs en la soledad en escolares
**Link:**
https://www.youtube.com/watch?v=LKdMsaIFN4s

## Ciberdelitos: ¿Donde solicitar asesoramiento?

• 911 de la Policía.

• Ministerio Público de Salta (Ciudad Judicial):
  • Teléfono : (0387) 4-258000
  • Mail: contactompf@mpublico.gov.ar
  • Oficina de Orientación y Denuncia: http://www.mpfsalta.gov.ar/OOyD/Oficina-de-Orientacion-y-Denuncia

• Unidad Fiscal Especializada en Ciberdelincuencia :
  • Teléfono : (+5411) 5471-0040
  • Mail: denunciasufeci@mpf.gov.ar

• División Delitos Tecnológicos de la Policía Federal Argentina:
  • Teléfono : (+5411) 4800-1120 / 4370//-5899
  • Mail: delitostecnologicos@policiafederal.gov.ar

• Fiscalía de Primera Instancia N° 1 de Salta:
  • Teléfono: (0387) 4-312313
  • Mail: fisfed1-sta@mpf.gov.ar

Poder Judicial de la Provincia de Salta
Av. Bolivia 4671 - CPA: A44008FVG
Teléfono: (0387) 4-258000
Web: http://www.justiciasalta.gov.ar