Cibercrimen y delitos informáticos

> Apuntes para la materia

SUPERINTENDENCIA DE INSTITUTOS DE FORMACIÓN POLICIAL
SUBSECRETARÍA DE FORMACIÓN Y DESARROLLO PROFESIONAL
MINISTERIO DE SEGURIDAD
GOBIERNO DE LA PROVINCIA DE BUENOS AIRES

AÑO 2022

Resolución: D.G.C y E. 1011 del año 2017

Autoridades:

Gobernador de la Provincia de Buenos Aires

Dr. Axel Kicillof

Ministro de Seguridad de la Provincia de Buenos Aires
Dr. Sergio Berni

Subsecretario de Formación y Desarrollo Profesional
Tec. Javier Alonso

Director Provincial de Formación, Capacitación y Evaluación
Lic. Gonzalo García

Directora de Capacitación y Entrenamiento
Lic. Flavia Tello Cortez

Superintendente de Institutos de Formación Policial
Crio. Gral. Julio Adrián Poles

Directora de Planificación Educativa y Evaluación Institucional
Crio. Natalia González

Director de la Escuela Juan Vucetich
Crio. Mayor Rubén Peralta

Apuntes para la materia

Cibercrimen y delitos informáticos

Coordinación de contenidos:

Crio. Mayor Rubén Peralta

Crio (Prof) Gil Leandro

Participaron en la redacción del presente material:

Prof. Susana Fuentes

Prof. Lilian Nieto

Crio. Mayor (CDO) (RA) Juan Tedesco

Revisión

O.A Milohnic Gaspar

Diseño gráfico y diagramación

DG. Bruno Valentini

DG. Horacio Augusto Pagani

DG. Rodrigo Gonik

Contenido

A los fines de colaborar con la comprensión del siguiente material —el cual consta de transcripciones provenientes de diferentes códigos y reglamentaciones legales—, se permite la incorporación de determinados elementos de diseño que remarquen conceptos para facilitar la lectura de los mismos.

Dichas transcripciones se resaltarán con un cambio de tipografía —eligiéndose para tal fin la fuente Times New Roman—. Del mismo modo, los agregados de texto que fueren necesarios para agilizar la lectura y facilitar su comprensión/aprehensión—y sean de autoría del equipo docente a cargo del presente material— se realizarán entre corchetes ([ ]).

Introducción

El presente proyecto trata de lograr la mejor correspondencia entre éste y los contenidos del plan de estudio para que el alumno una vez egresado pueda resolver los problemas básicos que se le presentarán en su trabajo cotidiano. Se trata de incorporar a través del proceso de enseñanza-aprendizaje, que es continuo y constante, la resolución de casos puntuales ante los cuales deberán estar preparados. El alumno durante este proceso deberá lograr no aprender los contenidos en forma automática o por repetición sino a través de la práctica que es fundamental para su carrera profesional. Tratar de incorporarlos en forma gradual para poder utilizarlos adecuadamente, sin desconocer los conceptos teóricos que serán la base misma de este proceso.

Para lograr un mejor desarrollo del alumno el proceso debe ser flexible, con espacio abierto al diálogo y a la requisitoria efectuada tanto a nivel individual como grupal. Teniendo en cuenta los contenidos, se desea que a través del proceso de enseñanza aprendizaje el alumno tenga conocimientos básicos de informática, la regulación existente y la forma que deberá conducirse a fin de evitar la pérdida o daño de la prueba virtual, todo lo cual le permitirá al egreso saber comportarse ante una situación tanto en el ámbito laboral como en su vida cotidiana, aún con simples elementos que tenga a su alcance. Los recursos que se utilizarán son apuntes elaborados por el docente, gráficos en el pizarrón, material audiovisual, utilización de elementos básicos de informática, guías de lectura, recortes periodísticos, consultas en distintas páginas web oficiales, etc.

Unidad 1

> Nociones de informática

U1

Definición de informática

La informática se define como la ciencia que estudia el tratamiento de la información mediante medios automáticos, es decir la ciencia de la información automática.

Desde los primeros tiempos, el ser humano ha inventado y desarrollado medios necesarios para transmitir información: medios como el lenguaje, la escritura, las señales acústicas o luminosas como silbatos, tambores, humo, el teléfono, la televisión, pudiendo trasladar de generación en generación todo el pensamiento y conocimiento adquirido a lo largo de la historia, gracias a esta transmisión y tratamiento de la información el ser humano ha evolucionado hacia la tecnología que actualmente disponemos.

Para poder automatizar la información se necesitan realizar tres tareas básicas:

1. Entrada: captación de la información. Normalmente son datos y órdenes ingresadas por los usuarios a través de cualquier dispositivo de entrada conectado a la computadora.

2. Proceso: tratamiento de la información. Se realiza a través de programas y aplicaciones diseñadas por programadores que indican de forma secuencial cómo resolver un requerimiento.

3. Salida: transmisión de resultados. A través de los dispositivos de salida los usuarios pueden visualizar los resultados que surgen del procesamiento de los datos.

Función

1. Creación de nuevas especificaciones de trabajo

2. Desarrollo e implementación de sistemas informáticos

3. Sistematización de los procesos

4. Optimización de los métodos y sistemas informáticos existentes

Definición de hardware

Hardware son todos aquellos componentes físicos de una computadora, todo lo visible y tangible y se aplica a las plaquetas electrónicas, dispositivos electromecánicos y ópticos, etc.

El *hardware* realiza las cuatro actividades fundamentales: entrada, procesamiento, salida y almacenamiento secundario.

Definición de software

El *software* es la parte lógica de la PC, el *alma*, los programas, datos y la información que en ella se encuentra. Sin el software, la computadora sería un conjunto de elementos que no funcionarían. Cuando comienzan a correr los programas, este hardware recibe instrucciones básicas que le permitirán funcionar en forma lógica y coordinada, haciendo eficiente el uso del material.

Categorías

- Software de base o sistemas operativos: es aquel que proporciona programas cuya función principal es ayudar al funcionamiento y desarrollo de las labores del computador y de sus componentes

- Software de programación: conjunto de herramientas que permiten desarrollar programas informáticos usando diferentes alternativas y lenguajes de programación de manera práctica.

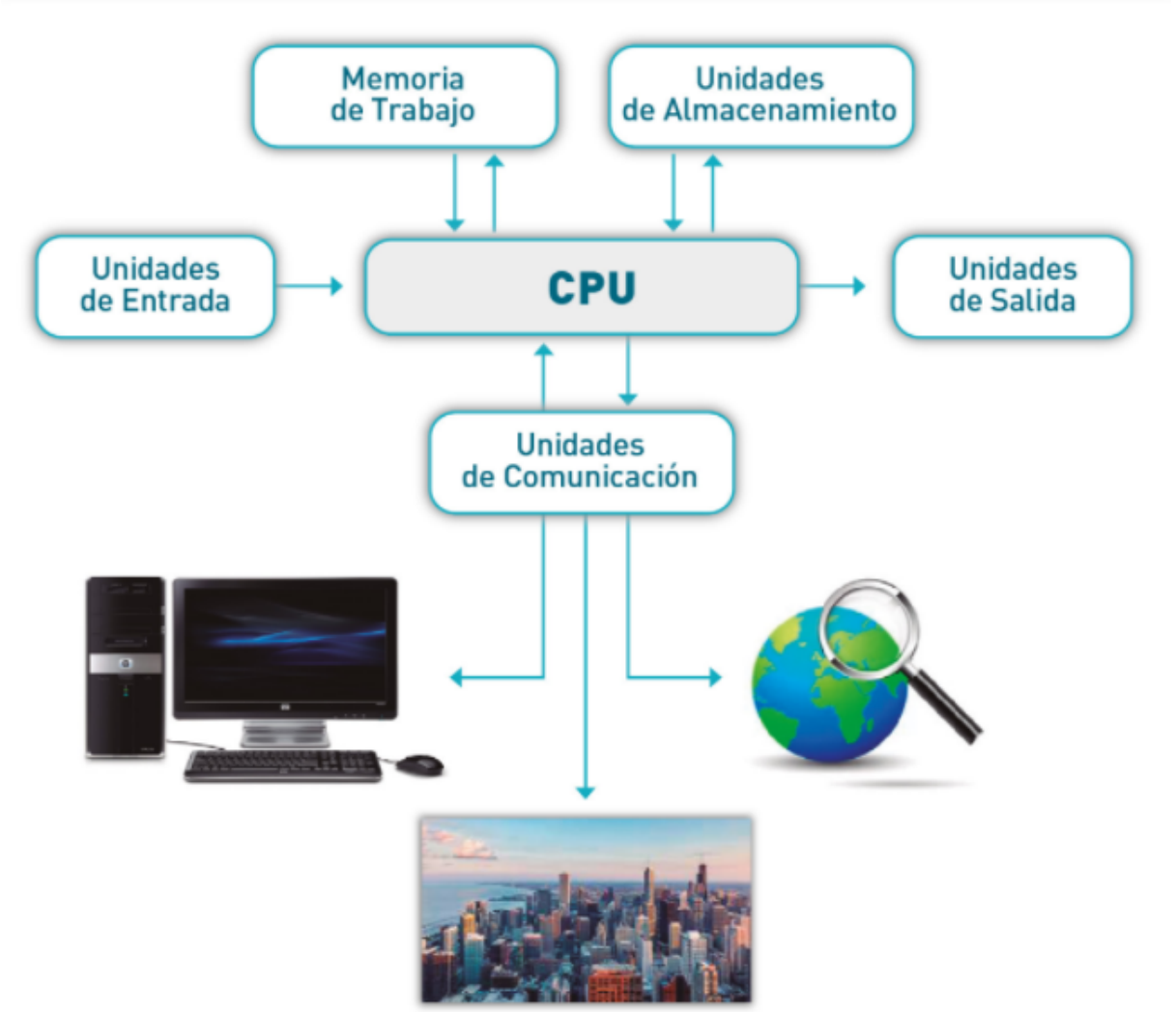
- Software de uso general: el software para uso general ofrece la estructura para un gran número de aplicaciones empresariales, científicas y personales. El software de hoja de cálculo, de diseño asistido por computadoras (CAD), de procesamiento de texto, de manejo de bases de datos, pertenece a esta categoría. La mayoría de software para uso general se vende como paquete; es decir, con software y documentación orientada al usuario (manuales de referencia, plantillas de teclado y demás).

- Software de aplicación: programa que facilita la realización de una tarea. Posee características propias, puede realizar tareas de uso general. Posee un lenguaje de programación propio. Se utiliza para la automatización de tareas complicadas

- Firmware: Se refiere a las rutinas de software almacenadas en memoria de sólo lectura (ROM). Las rutinas de inicio de la computadora y las instrucciones de entrada/salida

de bajo nivel se almacenan como firmware. En cuanto a la complejidad que supone modificarlo, el firmware se encuentra a medio camino entre el software y el hardware.

El ordenador



Si bien no podemos comparar a un computador con un ser humano, vamos a tomarnos ese atrevimiento. Imaginemos a un soldado bien entrenado que solo puede acatar órdenes y actuar en consecuencia. Un computador es un conjunto de piezas electrónicas preparadas para recibir órdenes, y actuar en consecuencia, al igual que el soldado, posee un *cerebro* denominado CPU (Unidad Central de Proceso), la cual ha sido dotada de un sistema operativo, lo que le da la capacidad de un lenguaje o una interfaz capaz de comunicarse con su entorno. Sería algo así como la formación o educación que recibió el soldado, -conocimiento indispensable para desarrollar las tareas-.

Está representado físicamente por un circuito electrónico. Posee dos unidades:

- **Unidad de control**: lugar donde se generan las instrucciones de control.
- **Unidad aritmética-lógica**: Toma los datos ingresados y los procesa a través de funciones lógico matemáticas informando el resultado.

Conociendo el interior de nuestro ordenador

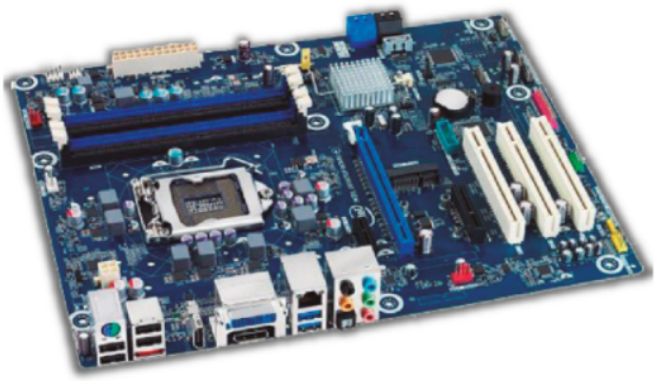
Si hacemos un breve recorrido por el interior de nuestro ordenador encontraremos elementos (hardware) muy importantes cuya función es la de encargarse de que todo funcione a la perfección. El desarrollo tecnológico actual permite que estos elementos físicos sean durables, con pocas posibilidades de que se rompan o dejen de funcionar.

La placa madre: el corazón de nuestra PC

Todos los circuitos electrónicos, los chips y otros componentes que existen en gran número en nuestra PC, se encuentran integrados en esta gran placa que recibe el nombre de *placa madre* o *motherboard*.

Recibe este nombre por ser el lugar que alberga el microprocesador, que es el responsable de que todo funcione a mayor o menor velocidad. Continuamente aparecen nuevos modelos con mejoras en la velocidad de trabajo, existiendo dos marcas principales: Intel y Amd

Además en esta placa encontramos diversas ranuras (llamadas puertos) que permiten la inserción de placas adicionales (de memoria RAM, por ejemplo), y para ampliar las prestaciones.



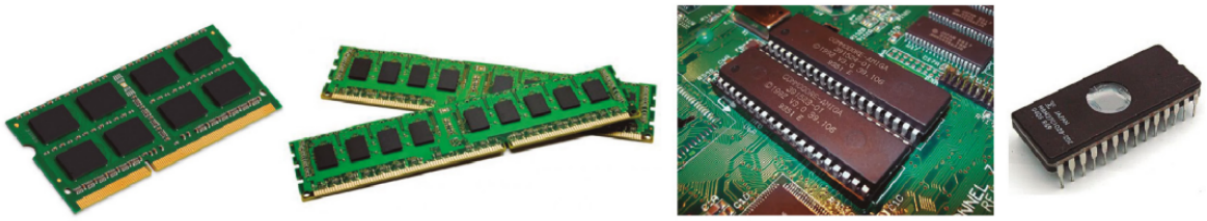
Definición de memoria

Son dispositivos capaces de retener datos informáticos durante algún intervalo de tiempo. Las memorias de computadora proporcionan una de las principales funciones de la computación moderna, la retención o almacenamiento de información.

Es uno de los componentes fundamentales de todas las computadoras modernas.

En la actualidad, memoria suele referirse a una forma de almacenamiento de estado sólido conocido como memoria RAM (memoria de acceso aleatorio, RAM por sus siglas en inglés *random access memory* y otras veces se refiere a otras formas de almacenamiento rápido pero no temporal. De forma similar se refiere a las formas de almacenamiento masivo como discos ópticos y tipos de almacenamiento magnético como discos duros y otros almacenamientos más lentos que las memorias RAM, pero de naturaleza más permanente

Además, se refleja una diferencia técnica importante y significativa entre memoria y dispositivos de almacenamiento masivo, que se ha ido diluyendo por el uso histórico de los términos *almacenamiento primario* (a veces *almacenamiento principal*), para memorias de acceso aleatorio, y *almacenamiento secundario* para dispositivos de almacenamiento masivo.



Tipos de memoria

Existen 3 tipos de memorias:

- **Memoria RAM** (Random access memory): se encuentra en el microprocesador y se utiliza para almacenar los programas o las instrucciones que le impartimos para que se lleve a cabo las operaciones. Es volátil, es decir, se vacía cuando se apaga el equipo. Se debe tener en cuenta que cuanto mayor sea la cantidad de memoria que tenga un ordenador, mayor número de operaciones puede llevar a cabo. Además, debido a la complejidad y a la cantidad de posibilidades que ofrecen los programas actuales, cada vez se hace necesario disponer de más memoria para que estos puedan trabajar adecuadamente.

- **Memoria ROM** (Random only memory): solo se utiliza para ser leída y posee pequeños programas que han sido almacenados por el fabricante, cuya función es el control del estado del ordenador. Los programas que posee almacenados tienen como misión

principal comprobar que todos los componentes del computador estén en buenas condiciones y que funcionan perfectamente: el teclado, el monitor, las unidades de almacenamiento, etc. Es fija y no puede borrarse. No desaparece cuando se apaga el ordenador. También almacena la fecha y la hora.

- **Memoria virtual**: técnica de gestión de la memoria que se encarga de que el sistema operativo disponga, tanto para el software de usuario como para sí mismo, de mayor cantidad de memoria que la que está disponible físicamente. Su objetivo es intentar que la información que está usando un proceso en un determinado momento (conjunto de trabajo) esté residente en memoria principal. Cuando varios trabajos se están procesando de manera concurrente, el sistema operativo debe controlar el modo en el que se está usando la memoria de la computadora y asegurarse de que ningún trabajo invade el espacio de otro.

El microprocesador: el trabajo duro de nuestro equipo

Es el encargado de controlar todo el sistema y también recibe el nombre de CPU (Unidad Central de Procesamiento). Como su propio nombre indica, es el que ***procesa*** todas y cada una de las instrucciones que recibe, en respuesta a lo que nosotros le pidamos a nuestro ordenador. Evidentemente, a más potencia del microprocesador, más rapidez en la ejecución de cualquier operación.

Cualquier tarea que realicemos en nuestro ordenador (desde pulsar una tecla, hasta realizar cálculos complicados), provocará una serie de instrucciones que siempre pasarán por este microprocesador el cual a velocidades de millonésimas de segundo enviará las instrucciones correctas en cada caso.

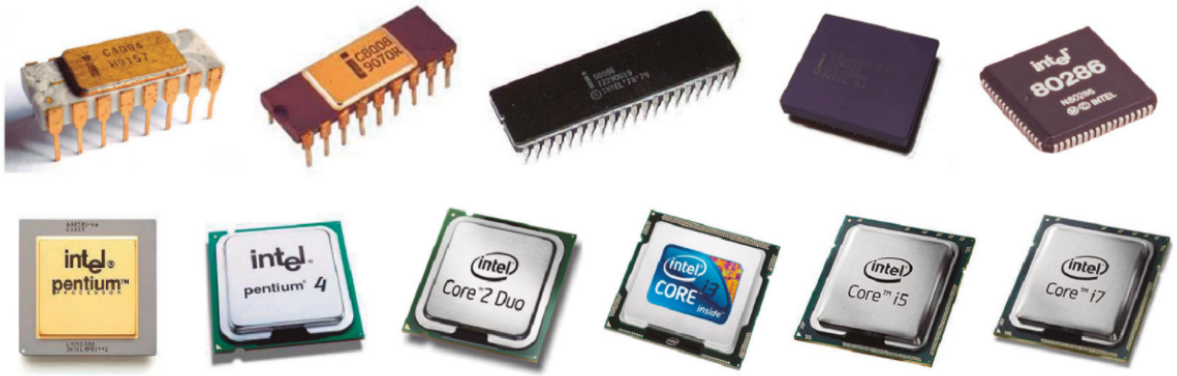
Existen dos compañías que se dedican a la fabricación de microprocesadores: Intel y AMD, siendo estos últimos algo más baratos que los Intel, pero con una eficacia probada que nada tiene que envidiar a los de la otra marca.

Como curiosidad decir que las velocidades actuales de las CPU o microprocesadores, se miden en Gigahercios (GHz). Para tener una idea, una CPU con 1 GHz funciona a una velocidad de unos mil millones de ***tics de reloj*** ¡¡por segundo!! Se deduce por tanto que mientras más Gigahercios tenga un microprocesador, mayor será la velocidad de trabajo en el procesamiento de las tareas que realice.

Todos los microprocesadores llevarán siempre acoplado un sistema de disipación de calor (ventilador y otros sistemas) debido a que se producirán unas elevadas temperaturas cuando trabaja.

Últimamente podemos encontrar micros de doble núcleo e incluso de cuádruple núcleo que como habrás adivinado son inventos que permiten duplicar o cuadruplicar la

velocidad de trabajo de la CPU. Se usan en trabajos exigentes tales como la edición de vídeo y otros que tú seguramente no realizarás.



Definición de unidad central de proceso (CPU) o (UCP)

La Unidad Central de Proceso (UCP o CPU) se podría definir como el **cerebro del ordenador** (en el caso de una computadora), este dispositivo es el que se ocupa de controlar y gobernar el ordenador. Consiste en un circuito microscópico que interpreta y ejecuta las instrucciones de los programas almacenados en memoria y que además toma los datos de las unidades de salida, es decir, se trata del componente del ordenador que se ocupa del control y el proceso de datos.

Está formado por:

- La Unidad de Control (UC), que interpreta y ejecuta las instrucciones de la máquina almacenadas en la memoria principal o RAM (random acces memory) y genera señales de control necesarias para ejecutar dichas instrucciones.

- La Unidad Aritmético Lógica (UAL o ALU), que recibe los datos sobre los que efectúa operaciones de cálculo y comparaciones, toma decisiones lógicas (determina si una afirmación es correcta o falsa mediante reglas del álgebra de Boole) y devuelve luego el resultado, todo ello bajo supervisión de la unidad de control.

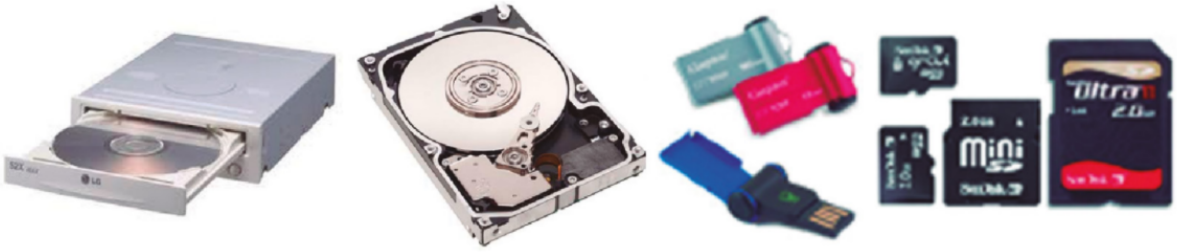
Las unidades de disco: un almacenamiento eficaz de larga duración

Uno de los errores en los que con más frecuencia incurren los usuarios de computadoras es confundir a la memoria RAM de la PC con un medio de almacenamiento,

pero esto no es así ya que la RAM sólo almacena datos temporalmente y con fines de que sean procesados por la CPU, nunca guardará datos en forma permanente.

Básicamente, una unidad de almacenamiento es un dispositivo capaz de leer y escribir información con el propósito de almacenarla permanentemente. En la actualidad contamos con muchas clases y categorías de unidades de almacenamiento, pudiendo encontrar en el mercado una amplia variedad de dispositivos internos o externos capaces de almacenar una cantidad de datos impensada en el pasado.

También llamado almacenamiento secundario, estos dispositivos pueden guardar información en su interior, como en el caso de los discos rígidos, tarjetas de memoria y pendrives, o como en el caso de las unidades de almacenamiento óptico como las lectograbadoras de Blu- Ray, DVD o CD, grabándolas en un soporte en forma de disco.



Este tipo de dispositivos es la más segura y práctica forma de almacenar muchísima cantidad de información en forma sencilla y permanente, además, los datos que guardemos en ellos siempre estarán disponibles gracias a que no es necesario suministrarles energía eléctrica para que permanezcan almacenados.

Dispositivos de almacenamiento

Son dispositivos electromecánicos basados en medios óptico-magnéticos que permiten guardar la información en forma permanente.

Si bien existen dispositivos que aplican distintas tecnologías (escritura sobre platillos magnéticos flexibles, rígidos, huellas ópticas, cintas magnéticas, etc.), podemos destacar el almacenamiento en forma de archivo, mediante la agrupación en carpetas o directorios.

Tipos de dispositivos de almacenamiento

- Medios Ópticos: CD, DVD, Blu-Ray etc.
- Medios Magnéticos: discos rígidos cintas magnéticas, diskettes, etc.

- Medios electrónicos: Discos SSD, Pendrive, tarjetas de memoria, etc.:
- Medios On Line:

- **Nube**: procesamiento y almacenamiento masivo de datos en servidores. Servicios que guardan la información en internet de la misma red y del usuario que lo solicite. Permite el acceso instantáneo desde cualquier dispositivo desde cualquier punto geográfico a través de dispositivos fijos (ordenadores, etc.) como dispositivos móviles (teléfonos inteligentes, tabletas, etc.). Uno de los ejemplos más claros de su uso el correo electrónico a través de tu navegador. Cuando vos accedés a tu e-mail (Hotmail o Gmail, por ejemplo) tenés la información en Internet a la que podes acceder de manera rápida. Lo único que hay que hacer es ingresar a un sitio, poner una clave y listo: podes acceder a todos tus correos, contactos y archivos adjuntos alojados en servidores de las diferentes empresas.

- **Dorpbox**: permite alojar cualquier archivo en la nube, sincronizar archivos de manera on line entre ordenadores, para poder compartir archivos y carpetas. Con Dropbox es posible sincronizar una carpeta de tu ordenador entre distintos dispositivos como un Android, Windows Phone, IOS, Mac, Windows, Linux.

- **Google drive**: Es el servicio de almacenamiento de datos en una nube de la red. El servicio incluye 15 GB gratuitos en una plataforma en la que puedes crear carpetas y guardar todo tipo de archivos. Con Drive, se tiene acceso a un escritorio en el que puedes organizar tus ficheros y básicamente hacer todas las funciones de una carpeta como las que se pueden hacer en el ambiente del sistema operativo que tiene la PC.

Definición de dispositivos periféricos, tipos y ejemplos

Los dispositivos periféricos son una serie de accesorios y componentes destinados a aumentar los recursos y posibilidades de un ordenador o dispositivo informático. Se instalan en base a diversos procesos dependiendo del tipo de periférico que se trate, pudiendo introducirse por una conexión USB, bluetooth o colocándolo con una instalación en el interior.

Los periféricos no se consideran indispensables para el funcionamiento y rendimiento de un ordenador, pero aportan una serie de funcionalidades básicas a la hora de usar los equipos informáticos.

Tienen la finalidad de aportar usos cotidianos y necesarios, como la introducción de contenido de texto a través de un teclado, o el movimiento del cursor del ordenador apoyándose en un ratón. Si bien por regla general se considera estos dispositivos como herramientas innecesarias, su utilización se ha convertido en algo imprescindible para sacar el máximo partido a los equipos informáticos de la actualidad.

Se clasifican en cinco categorías:

Periféricos

- Periféricos de entrada: es todo dispositivo cuya única función es ingresar información a la CPU. Es decir captan y envían los datos al dispositivo que los procesara. Los dispositivos más comunes son: el teclado, mouse, micrófono, cámaras fotográficas, scanner, etc.

- Periféricos de salida: todo dispositivo que recibe información de la CPU en forma exclusiva. Son dispositivos que muestran y proyectan información, hacia el exterior del ordenador, la mayoría son para informar, alertar, comunicar, proyectar o dar al usuario cierta información. De la misma forma se encargan de convertir los impulsos eléctricos en información legible para el usuario. Los dispositivos más comunes son: el monitor, impresoras, parlantes, proyectores, fax, etc.

- Periféricos de entrada y salida: sirven básicamente para la comunicación de la computadora con el medio externo. Los dispositivos más comunes son: PenDrive, multifunción, disco extraíble.

- Periféricos de almacenamiento: Son los dispositivos que almacenan datos de información por bastante tiempo, la memoria RAM no puede ser considerada un periférico de almacenamiento ya que su memoria es volátil y temporal. Los dispositivos más comunes son: Disco duro, unidad de CD, PenDrive, etc.

- Periféricos de comunicación: es todo dispositivo que conecta a la CPU con el mundo exterior. Se encargan de comunicarse con otras máquinas o computadoras, ya sea para trabajar en conjunto o para enviar o recibir información placas de red. Existen varias técnicas de conexión, entre ellas se destacan:

    - **MODEM**: es un dispositivo que permite un enlace con la línea telefónica. El nombre proviene de su función modulador-demodulador, convierte la información en pulsos eléctricos que envía a través del cable telefónico, controla el enlace y reconvierte los pulsos eléctricos en información.

- **ETHERNET**: es una tarjeta o plaqueta que nos permite el enlace con una red de área local (LAN).
- **USB**: es una puerta de enlace con periféricos de todo tipo. Su nombre proviene de Bus Serial Universal. Es el enlace favorito del momento, ya que es rápido, versátil y permite el auto detección de los dispositivos que a él se conectan.
- **SERIAL**: puerto de comunicación utilizado para conectar mouse, modem, terminales, impresoras y otros dispositivos. Su aplicación está cayendo en desuso. También se lo puede utilizar para conectarse con otra PC. Se lo considera lento. Actualmente está siendo reemplazado por el USB.
- **PARALELO**: puerto de comunicación normalmente utilizado para impresoras, escanners, enlaces con otras PCs. Es más rápido que el serial pero actualmente está siendo reemplazado por el USB.

Definición de explorador de archivos

Es una aplicación para administrar archivos que forma parte del sistema operativo Microsoft Windows. A través de esta herramienta es posible crear, editar o eliminar carpetas, archivos, etc.

Definición de internet

Se conoce como internet (INTERnationalNETwork), a una red de conexiones a través de la cual se comunican de forma descentralizada las computadoras, esto con ayuda de una serie de protocolos a los que se les denomina TCP/IP. El internet tiene sus inicios en la década de los 70, como medio de comunicación gubernamental en caso de producirse una guerra atómica.

Técnicamente el internet se puede definir como un grupo de redes de ordenadores que se encuentran interconectadas, pero su funcionamiento no se adapta a un solo tipo de ordenador, a un medio físico privilegiado, a un tipo de red en concreto, y ninguna tecnología inclusiva de conexión, ya que se trata de una red dinámica y flexible, que puede ser adaptada a distintos contextos tecnológicamente hablando.

Estas redes son por sí solas un universo de la tecnología, en donde convergen diversas ramas como la telefonía, microprocesadores, fibra óptica, satélites electrónica video, televisión, imágenes, realidad virtual, hipertexto, entre otras.

Correo electrónico o e-mail

El correo electrónico (también conocido como *e-mail*, un término inglés derivado de *electronic mail*) es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos. Los mensajes de correo electrónico posibilitan el envío, además de texto, de cualquier tipo de documento digital (imágenes, videos, audios, etc.)

El funcionamiento del correo electrónico es similar al del correo postal. Ambos permiten enviar y recibir mensajes, que llegan a destino gracias a la existencia de una dirección. El correo electrónico también tiene sus propios buzones: son los servidores que guardan temporalmente los mensajes hasta que el destinatario los revisa.

El estadounidense Ray Tomlinson fue quien incorporó el arroba (@) a las direcciones de correo electrónico, con la intención de separar el nombre del usuario y el servidor en el que se aloja la casilla de correo. La explicación es sencilla: @, en inglés, se pronuncia *at* y significa *en*.

Por ejemplo: carlos@servidor.com se lee Carlos at servidor.com (o sea, Carlos en servidor. com)

Además de todo lo expuesto tenemos que dar a conocer cuál es la estructura básica que tiene cualquier correo electrónico. Así, nos encontramos con los siguientes elementos básicos:

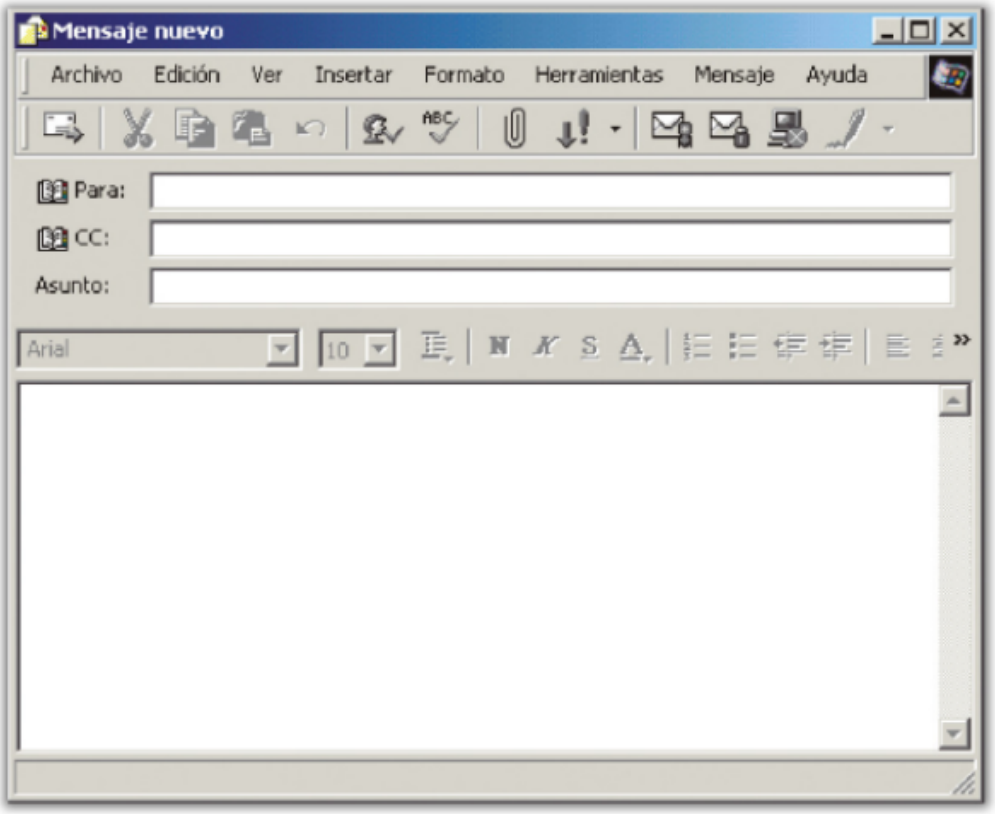
- **El destinatario,** en esta casilla llamada *para*, se pueden incluir tanto una como varias direcciones de personas a las que se les va a enviar dicho correo como principales destinatarios. Además se otorga la oportunidad de que esas direcciones que se van a incluir no sean visibles por el resto de personas que las reciben.

- ***CC***, el cual significa ***con copia***. La función que cumple el e-mail enviado con copia (CC) se muestra cuando queremos enviar el mail a varias personas, separando con comas a cada una de las direcciones de correo, por ej.: morticio@hotmail.com, anibalcanibal@live.com, etc. Entonces cuando cada una de las personas abre el mail, puede ver a quién ha sido enviado el correo, de esa manera puede ver cada una de las direcciones que han recibido el mail y agregarlas, como comúnmente pasa.

▸ ***CCO***, que significa ***con copia oculta***. La función que cumple este gran amigo desconocido es similar a la del ya mencionado CC, pero con la diferencia de que cuando nuestros destinatarios reciban el correo, no podrán ver a quién más ha sido enviado. De ésta manera logramos poner a salvo a nuestros queridos contactos y evitamos causar diferentes molestias, las que pueden ir desde facilitar direcciones de correo a desconocidos, hasta darle direcciones de correo servidas en bandeja de plata a *spammers*.

▸ El **asunto** es el apartado donde de manera breve y escueta debe aparecer el tema sobre el que gira el correo electrónico.

▸ El **mensaje.** En dicho apartado, de gran amplitud, es donde se escribe el mensaje que desea enviar. Para que dicho texto esté, estéticamente hablando, tal y como deseamos se ofrecen herramientas con las que elegir el tipo de letra, la alineación, el color, hipervínculos e incluso emoticones.



No obstante, tampoco podemos pasar por alto que a la hora de enviar un correo electrónico también y además del citado texto, y tal como hemos subrayado anteriormente, podemos incorporar diversos materiales o archivos. Eso supone que podamos adjuntar tanto documentos de diversa tipología (textos, hojas de cálculo, base de datos, pdf…) como fotografías e incluso vídeos.

Luego, quien reciba dicho e-mail tiene distintas posibilidades. Así, no sólo podrá leerlo y responderle al emisor del mismo sino que también podrá reenviarlo a otros destinatarios,

archivarlo, borrarlo de manera permanente, marcarlo, añadirle etiquetas y también catalogarlo como spam.

Cuando alguien envía un correo, primero llega a su servidor que lo envía al servidor del destinatario, el mensaje queda almacenado en el buzón del destinatario. Cuando el destinatario se conecte al servidor, éste le enviará todos sus mensajes pendientes. Por esto da igual que el destinatario esté conectado o no a Internet en el momento que se le envía un mensaje.

Podemos configurar nuestro correo para que cada vez que se arranque lea los mensajes pendientes o para que los lea cuando pulsemos en el botón ***recibir***.

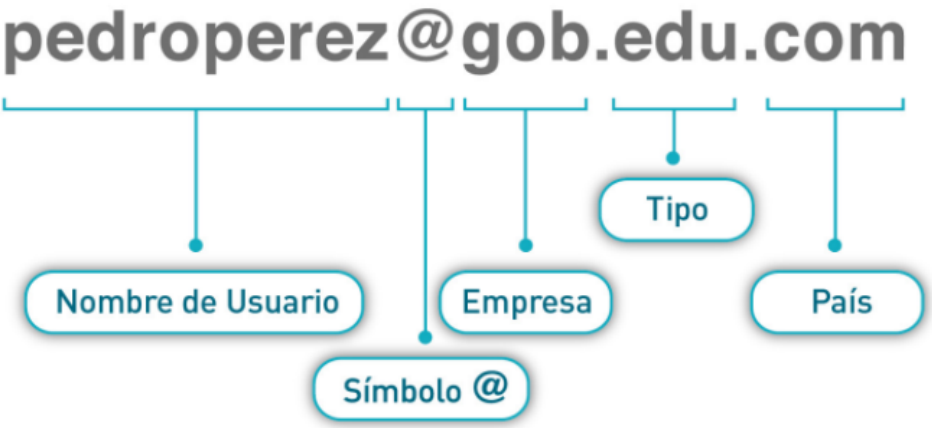
El servidor que alberga los correos suele disponer de un espacio limitado. Si en algún momento detecta que vas a sobrepasar dicha capacidad, recibirás un aviso para eliminar correos. Si no lo haces, tu bandeja de entrada no admitirá correos nuevos. De todas formas esto no debe preocuparte demasiado, porque hoy en día los principales servicios de correo electrónico ofrecen espacio de varios GB, que resulta más que suficiente en la mayoría de casos.

Direcciones de correo y sistema de envío

Una dirección de correo electrónico, o dirección e-mail, contiene el identificador del destinatario, así como el del servidor que recibirá el correo. El formato de una dirección de correo electrónico es similar a nombre@unad.edu.ar, donde el nombre será el identificador de la cuenta de correo electrónico, del destinatario y los demás caracteres que se encuentran después del símbolo @ es el nombre de la empresa de donde se deriva la cuenta, además del tipo de sitio y el país, es decir se escribiría todo el texto que va después de la sigla www del formato de una dirección electrónica de página Web.

El nombre será utilizado por el servidor para conocer quién deberá recibirlo y almacenarlo en su buzón correspondiente.

Ejemplo de dirección de correo electrónico



Virus informáticos

Un virus informático es un programa malicioso que se introduce en un ordenador, sin permiso o sin conocimiento de su usuario, para alterar su funcionamiento y, particularmente, con la finalidad de modificar o dañar el sistema. Por norma general, se asocian a un archivo ejecutable, quedando el equipo infectado cuando se abre dicho archivo. Para librarnos de tales amenazas, por fortuna, podemos hacernos con uno de los potentes antivirus que existen en el mercado.

Las aplicaciones malintencionadas, por tanto, ocasionan daños en los dispositivos, tanto en el hardware, como, otras veces, en el software. En el primer caso, un virus puede perjudicar el disco duro reduciendo su rendimiento y efectividad, quemar el microprocesador o estropear el sistema básico de entrada/salida (BIOS), entre otros problemas. Respecto al software, este tipo de programas maliciosos pueden modificar y eliminar programas y archivos, ralentizar el funcionamiento del sistema operativo, robar información confidencial, y datos del usuario o afectar a la conexión a internet.

Estos virus, se camuflan bajo diferentes formas en principio de apariencia inofensiva, como el archivo de un programa o un documento, pero que esconde un software peligroso. Un virus se puede ir propagando a través de las redes, pasando de un ordenador a otro, o bien se activa cuando el usuario ejecuta, sin darse cuenta, su instalación.

A continuación presentamos los lugares de contagio más frecuentes:

- Las redes sociales se han convertido en un campo muy propicio para los desarrolladores de estas amenazas.

- Los sitios web fraudulentos; aunque también existen los que, pese a ser legítimos, se hallan infectados.

PARA PENSAR

argas con regalo pueden traducirse en la instalación de un virus, ya que, en muchas ocasiones, detrás de mensajes como “Haz clic y obtén 1.000 euros” se puede esconder la ejecución de un programa malicioso.

- La entrada de dispositivos que están infectados, como son memorias USB, CD o DVD.

- La apertura de archivos adjuntos que se hallan en el correo no deseado, también conocido como SPAM.

El primer Virus de la historia fue denominado “Creaper” por sus creadores, lo que significa “enredadera” en español. Apareció atacando algunos ordenadores en el año 1972, y en la pantalla podía leerse un mensaje estilo “I`m a creaper, catch me if you can”. Como curiosa contrapartida, se desarrolló entonces el primer sistema antivirus, que para seguir un poco el juego propuesto, se denominó “Reaper”, es decir “segadora”.

Definición de antivirus, los más utilizados

Se denomina antivirus a un software utilizado para eliminar programas elaborados con intención destructiva. Así, los antivirus surgieron como una solución a la proliferación de software malicioso cuando el uso de computadoras personales comenzó a masificarse y con ello surgió todo un nuevo mercado.

Un virus informático tiene como finalidad principal alterar el funcionamiento de la computadora a espaldas del usuario. El espectro de virus existentes exhibe desde programas capaces de borrar los datos de la computadora, hasta algunos que solo causan molestias. Los virus informáticos carecen de la capacidad de auto replicarse, precisan de un software que sirve de huésped; cuando este se ejecuta, el virus se levanta en la memoria RAM, comienza a manejar programas del sistema operativo e infectar los archivos ejecutables que se utilicen, grabándose de modo definitivo en el disco rígido.

Los antivirus más utilizados y seguros de la actualidad son:

- 1. AVAST
- 2. Microsoft
- 3. ESET
- 4. Symantec
- 5. Avira
- 6. AVG
- 7. Kapersky
- 8. McAfee
- 9. Trend Micro
- 10. Panda

Sistemas operativos

En informática se denomina ***sistema operativo*** al conjunto de programas informáticos que permiten una satisfactoria administración de los recursos que necesita una computadora.

También conocido como software de sistema, el sistema operativo comienza a funcionar en la computadora inmediatamente después de encenderla y gestiona el software desde los niveles más básicos permitiendo además la interacción con el usuario.

Si bien el concepto se encuentra instalado a instancia de las computadoras, vale destacar que hay sistemas operativos que funcionan en la mayoría de los dispositivos electrónicos que emplean un microprocesador, como teléfonos celulares, consolas de juegos, etc.

En el sistema operativo se cumplen cinco funciones básicas:

a. Administración de recursos: permite al usuario la utilización del hardware, incluyendo los periféricos y el uso de las redes.

b. Suministro de interfaz a los usuarios: permite la carga de programas, el acceso a los archivos y la realización de otras tareas en la computadora.

c. Administración de archivos: permite crear, modificar y eliminar archivos.

d. Servicio de soporte y utilidades: permite la actualización, la incorporación de nuevas y más utilidades, mejora la seguridad del sistema en función de las necesidades, controla los nuevos periféricos que ingresan y corrige los errores que suceden en algunos software.

e. Administración de tareas: facilita la administración de todas las tareas informáticas que lleva a cabo el usuario.

Existen varios sistemas operativos actualmente, entre los más populares se destacan:

1. Windows, creado por Microsoft en el año 1981. Funciona en los ordenadores con procesadores Intel y AMD (los más comunes).Cubre la gran mayoría de las necesidades del usuario. Es fácil de usar y configurar. Tiene fama de inestable ya que se bloquea o cuelga frecuentemente. No es muy seguro, ya que sus fallos permiten el ingreso de virus.

2. Mac OS, creado por Apple para sus computadoras Macintosh. Es considerado como el sistema operativo más sencillo de usar, más innovador y de mejor estética.

3. Linux, es un sistema operativo semejante a Unix, de código abierto y desarrollado por una comunidad para computadoras, servidores, mainframes, dispositivos móviles y dispositivos embebidos.

Software de aplicaciones

Procesador de texto

Es una aplicación que permite crear y editar documentos de texto en una computadora. Se trata de un software de múltiples funcionalidades para la redacción, con diferentes tipografías, tamaños de letra, colores, efectos artísticos y otras opciones.

Los procesadores de texto realizan una función similar a las viejas máquinas de escribir, aunque mucho más completa y compleja. Es posible borrar y editar el contenido sobre la pantalla. Una vez finalizada la tarea el usuario puede guardar el documento en soporte digital o en papel.

Los procesadores permiten intercalar imágenes y gráficos dentro del texto. Microsoft Word, es uno de los procesadores de texto más populares.

Planilla u hoja de cálculo

La hoja de cálculo es una herramienta informática que se utiliza para realizar cálculos, operaciones lógicas y manejo de datos. Al usuario se le presenta como un conjunto

de columnas y filas identificable por letras y números respectivamente, que van formando celdas. Su uso se orienta a actividades que requieren muchos cálculos en paralelo.

Las operaciones básicas que una hoja de cálculo utiliza son: suma, resta, multiplicación y división. Existe una amplia gama de posibilidades en lo que respecta a funciones de cálculos más complejos.

Estas planillas son documentos compuestos de datos numéricos y alfanuméricos dispuestos en tablas. Éstos pueden ser creados, editados y visualizados con distintos programas, permitiendo realizar operaciones matemáticas, crear tablas dinámicas, dibujar gráficos y otras cosas más.

Celda: unidad básica que permite el ingreso de datos. Está identificada por la columna (letras) y fila (números) donde se encuentra.

El Microsoft Excel es uno de los más conocidos.

Gestor de base de datos

Se define como el conjunto de programas que administra y gestiona la información contenida en una base de datos. Ayuda a realizar las siguientes acciones:

- Definición de los datos
- Mantenimiento de la integridad de los datos dentro de la base
- Control de la seguridad y privacidad de los datos
- Manipulación de los datos

Se trata de un conjunto de programas no visibles al usuario que se encarga de la privacidad, la integridad, la seguridad de los datos y la interacción con el sistema operativo. Proporciona una interfaz entre los datos, los programas que lo manejan y los usuarios finales.

Es necesario contar con un usuario administrador encargado de centralizar las tareas.

Gestor de comunicaciones

Se utiliza para establecer la comunicación entre dos o más computadoras en diferentes lugares. Permite enviar y recibir información mediante correo electrónico y mensajes instantáneos, como así también el acceso a bases de datos.

Programación para presentaciones

PowerPoint es el nombre de uno de los programas más populares. Se trata de un software que permite realizar presentaciones a través de diapositivas.

El programa contempla la posibilidad de utilizar textos, imágenes, música y animaciones. De este modo, la creatividad del usuario resulta decisiva para que las presentaciones sean atractivas y consigan la atención del receptor.

Se utilizan para dictar clases, lanzar productos o comunicar ideas.

Programación de diseños vectorizados

El término vectorial es usado regularmente en diseño para definir un tipo de gráfico de dos direcciones producidas mediante un computador y un software especializado. Son programas que crean gráficos usando formas geométricas básicas (línea, punto). Los gráficos pueden ser simples o complejos.

Ejemplos: Adobe Illustrator, Autocad, Corel Draw, etc.

Programación con mapa de bits

Se trata de aquellas imágenes que se forman a partir de puntos, llamados pixeles, dispuestos en un rectángulo o tabla. Cada píxel contiene la información del color.

De acuerdo a la cantidad de píxeles incluidos en el mapa de bits queda determinada la resolución de la imagen. Es muy común oír 1280x720, 1920x1080 que representan el número de puntos definidos por el ancho y por el alto.

Redes

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP, concibe cada red estructurada en cuatro capas con funciones concretas pero relacionadas entre sí Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

La comunicación por medio de una red se lleva a cabo en dos diferentes categorías:

- La capa física incluye todos los elementos de los que hace uso un equipo para comunicarse con otros equipos dentro de la red, como, por ejemplo, las tarjetas de red, los cables, las antenas, etc.

- La comunicación a través de la capa lógica se rige por normas que permiten construir los denominados protocolos, (normas de comunicación más complejas), capaces de proporcionar servicios que resultan útiles. Los protocolos son un concepto muy similar al de los idiomas de las personas. Si dos personas hablan el mismo idioma, y respetan ciertas reglas (tales como hablar y escucharse por turnos), es posible comunicarse y transmitir ideas/ información.

1. Componentes básicos de las redes

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos:

- Dispositivos de usuario final (hosts): incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario

- Dispositivos de red: son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es interconectar los componentes hardware de una red, y por tanto, principalmente, los ordenadores individuales, también denominados hosts, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado (o tecnología inalámbrica) soportada por la electrónica de red y unidos por cableado (o radiofrecuencia).

En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (Ethernet, Wi-Fi, Bluetooth, etc.)

Software

- **Sistema operativo de red**: permite la interconexión de ordenadores para acceder a los servicios y recursos. Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. En muchos casos el sistema operativo de red es parte del sistema operativo de los servidores y de los clientes.

- **Software de aplicación**: todos los elementos se utilizan para que el usuario de cada estación pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correos electrónicos, etc.

Hardware

Para lograr el enlace entre los ordenadores y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red (NIC, Network interface controller), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otros ordenadores, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, -ceros y unos-).

Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

Middleware

El término middleware se refiere a un sistema de software que ofrece servicios y funciones comunes para las aplicaciones. En general, el middleware se encarga de las tareas de gestión de datos, servicios de aplicaciones, mensajería, autenticación y gestión de API.

Ayuda a los desarrolladores a diseñar aplicaciones con mayor eficiencia. Además, actúa como hilo conductor entre las aplicaciones, los datos y los usuarios.

En el caso de las empresas con entornos de contenedores y multicloud, el middleware puede rentabilizar el desarrollo y la ejecución de aplicaciones a escala.

Dispositivos de usuario final

- **Ordenadores personales**: son los puestos de trabajo habituales de las redes. Dentro de la categoría de ordenadores, y más concretamente ordenadores personales, se engloban todos los que se utilizan para distintas funciones, según el trabajo que realizan

- **Terminal**: muchas redes utilizan este tipo de equipo en lugar de puestos de trabajo para la entrada de datos. En estos solo se exhiben datos o se introducen. Este tipo de terminales, trabajan unido a un servidor, que es quien realmente procesa los datos y envía pantallas de datos a los terminales.

- **Electrónica del hogar**: los adaptadores de red empezaron a integrarse en muchos elementos habituales de los hogares: televisores, equipos multimedia, proyectores, videoconsolas, teléfonos celulares, libros electrónicos, etc. e incluso en electrodomésticos, como frigoríficos o equipos de aire acondicionado, convirtiéndolos en partes de las redes junto a los tradicionales ordenadores.

- **Impresoras**: muchos de estos dispositivos son capaces de actuar como parte de una red de ordenadores sin ningún otro elemento, tal como un *print server*, actuando como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión determinado.

- **Otros elementos**: escáneres, lectores de CD-ROM.

Servidores

Son los equipos que ponen a disposición de los usuarios los distintos servicios. En la siguiente lista hay algunos tipos comunes de servidores y sus propósitos:

- **Servidor de archivos**: almacena varios tipos de archivo y los distribuye a otros clientes en la red.

- **Servidor de impresión**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión

- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con el correo electrónico (e-mail) para los clientes de la red.

- **Servidor de fax**: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax, con origen y/o destino una ordenador o un dispositivo físico de telefax.

- **Servidor de telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o Internet, etc.

- **Servidor proxy**: realiza un cierto tipo de funciones en nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones. También «sirve» seguridad; esto es, tiene un firewall (cortafuegos). Permite administrar el acceso a Internet en una red de ordenadores permitiendo o negando el acceso a diferentes sitios web, basándose en contenidos, origen/destino, usuario, horario, etc.

- **Servidor de acceso remoto** (Remote Access Service, RAS): controla las líneas de módems u otros canales de comunicación de la red para que las peticiones conecten una posición remota con la red, responden las llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red. Gestionan las entradas para establecer las redes virtuales privadas (VPN).

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material web compuesto por datos (conocidos normalmente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de streaming**: servidores que distribuyen multimedia de forma continua evitando al usuario esperar a la descarga completa del fichero. De esta forma se pueden distribuir contenidos tipo radio, vídeo, etc. en tiempo real y sin demoras.

- **Servidor de reserva** (standby server): tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red.

- **Servidor de autenticación**: es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable.

- **Servidores para los servicios de red**: estos equipos gestionan aquellos servicios necesarios propios de la red y sin los cuales no se podrían interconectar.

- **Servidor de base de datos**: permite almacenar la información que utilizan las aplicaciones de todo tipo, guardándola ordenada y clasificada y que puede ser recuperada en cualquier momento y sobre la base de una consulta concreta.

- **Servidor de aplicaciones**: ejecuta ciertas aplicaciones. Gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

- **Servidores de monitorización y gestión**: ayudan a simplificar las tareas de control, monitorización, búsqueda de averías, resolución de incidencias, etc.

Dispositivos de red

Los equipos informáticos descritos necesitan de una determinada tecnología que forme la red en cuestión. Los elementos de la electrónica de red más habituales son:

- Conmutador de red (switch),
- Enrutador (router),
- Puente de red (bridge),
- Puente de red y enrutador (brouter),
- Punto de acceso inalámbrico (Wireless Access Point, WAP).

Protocolos de redes

Existen diversos protocolos, estándares y modelos que determinan el funcionamiento general de las redes. Destacan el TCP/IP. Cada modelo estructura el funcionamiento de una red de manera distinta. El TCP/IP cuenta con cuatro capas diferenciadas pero que combinan las funciones existentes.

2. Clasificación de redes

Una red puede recibir distintos calificativos de clasificación sobre la base de distintas taxonomías: alcance, tipo de conexión, tecnología, etc.

a. Por alcance

- Red de área personal (Personal Area Network, PAN) es una red de ordenadores usada para la comunicación entre los dispositivos del ordenador cerca de una persona.

- Red inalámbrica de área personal (Wireless Personal Area Network, WPAN), es una red de ordenadores inalámbrica para la comunicación entre distintos dispositivos (tanto ordenadores, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal. El medio de transporte puede ser cualquiera de los habituales en las redes inalámbricas pero las que reciben esta denominación son habituales en Bluetooth.

- Red de área local (Local Area Network, LAN), es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión.

- Red de área local inalámbrica (Wireless Local Area Network, WLAN), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas.

- Red de área de campus (Campus Area Network, CAN), es una red de ordenadores de alta velocidad que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, una base militar, hospital, etc.

- Red de área metropolitana (Metropolitan Area Network, MAN) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero aun así limitado. Por ejemplo, una red que interconecte los edificios públicos de un municipio dentro de la localidad por medio de fibra óptica.

- Red de área amplia (Wide Area Network, WAN), son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como: satélites, cables interoceánicos, Internet, fibras ópticas públicas, etc.

b. Medios guiados

- Cable de par trenzado: es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la

potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares trenzados.

- Cable coaxial: se utiliza para transportar señales electromagnéticas de alta frecuencia, el cual posee un núcleo sólido (generalmente de cobre) o de hilos, recubierto por un material dieléctrico y una malla o blindaje, que sirven para aislar o proteger la señal de información contra las interferencias o ruido exterior.

- Fibra óptica: es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

c. Medios no guiados

- Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

- Red por infrarrojos (Infrared Data Association, IrDA), permiten la comunicación entre dos nodos, usando una serie de ledes infrarrojos para ello. Se trata de emisores/ receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan visibilidad entre los dispositivos.

- Red por microondas, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión.

d. Por relación funcional

- Cliente-servidor es la arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

- Peer-to-peer, o red entre iguales, es aquella red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

e. Por tecnología

- Red punto a punto (point to point, PtP) es aquella en la que existen multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en

algunos casos, máquinas intermedias que establezcan rutas para que puedan transmitirse paquetes de datos. El medio electrónico habitual para la interconexión es el conmutador, o switch.

- Red de difusión (broadcast) se caracteriza por transmitir datos por un solo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo. Los equipos unidos por un concentrador (hub), forman redes de este tipo.

- Red multipunto, dispone de una línea o medio de comunicación cuyo uso está compartido por todas las terminales en la red. La información fluye de forma bidireccional. Los terminales pueden estar separados geográficamente.

f. Por grado de autentificación

- Red privada: es una red que solo puede ser usada por algunas personas y que está configurada con clave de acceso personal.

- Red de acceso público: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de ordenadores interconectados, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

g. Por grado de difusión

- Una intranet es una red privada de ordenadores que utiliza tecnología de Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

- La Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

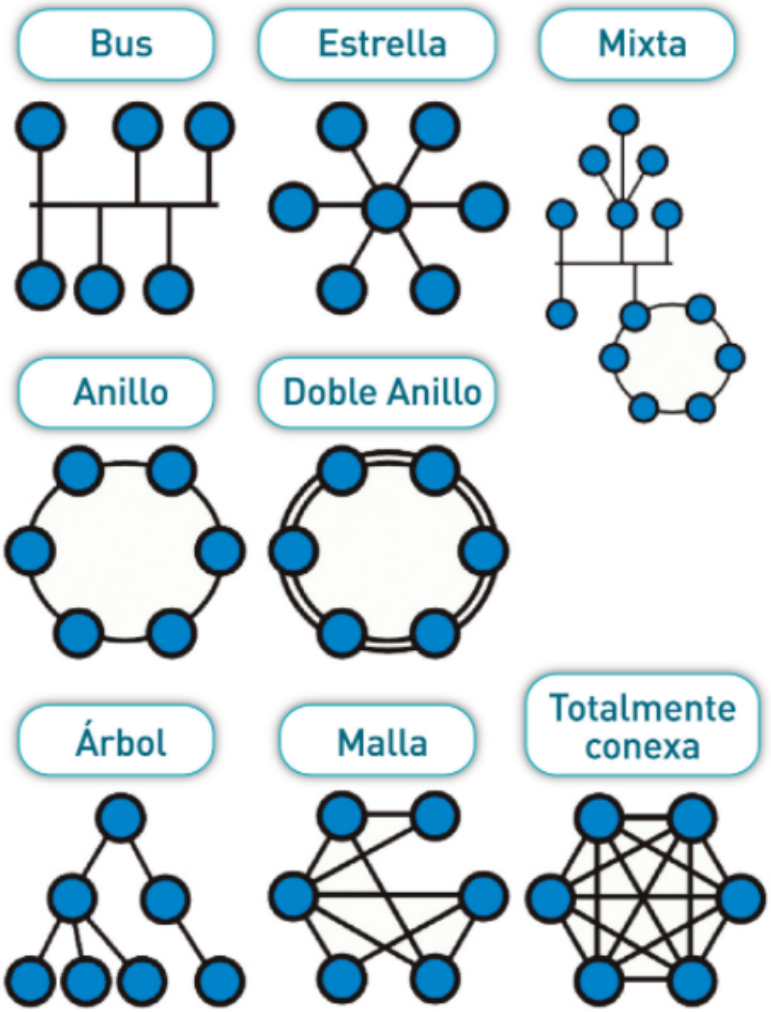
h. Por servicio o función

- Red comercial proporciona soporte e información para una empresa u organización con ánimo de lucro.

- Red educativa proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.

- Red para el proceso de datos proporciona una interfaz para intercomunicar equipos que vayan a realizar una función de cómputo conjunta.

i. Por topología física



- Red en bus (bus o «conductor común») o Red lineal (line): se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos.

- Red en anillo (ring) o Red circular: cada estación está conectada a la siguiente y la última está conectada a la primera. Además, puede compararse con la red en cadena margarita (daisy chain).

- Red en estrella (star): las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este.

- Red en malla (mesh): cada nodo está conectado a todos los otros.

- Red en árbol (tree) o red jerárquica: los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

- Red híbrida o red mixta: se da cualquier combinación de las anteriores. Por ejemplo, circular de estrella, bus de estrella, etc.

j. Por la direccionalidad de los datos

- Simplex o unidireccional: un equipo terminal de datos transmite y otro recibe.
- Half-duplex o semidúplex: el método o protocolo de envío de información es bidireccional pero no simultáneo bidireccional, solo un equipo transmite a la vez.
- Full-dúplex o dúplex: los dos equipos involucrados en la comunicación lo pueden hacer de forma simultánea, transmitir y recibir.

Página web

Una página web, o página electrónica, página digital, o ciberpágina es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes y muchas otras cosas, adaptada para la llamada World Wide Web (WWW) y que puede ser accedida mediante un navegador web. Esta información se encuentra generalmente en formato HTML o XHTML, y puede proporcionar acceso a otras páginas web mediante enlaces de hipertexto. Frecuentemente también incluyen otros recursos como pueden ser hojas de estilo en cascada, guiones (scripts), imágenes digitales, entre otros.

Las páginas web pueden estar almacenadas en un equipo local o en un servidor web remoto. El servidor web puede restringir el acceso únicamente a redes privadas, por ejemplo, en una intranet corporativa, o puede publicar las páginas en la World Wide Web. El acceso a las páginas web es realizado mediante una transferencia desde servidores, utilizando el protocolo de transferencia de hipertexto (HTTP).

Características y tipos de páginas

Una página web está compuesta principalmente por información de un tema factible (solo texto y/o módulos multimedia) así como por hiperenlaces; además puede contener o asociar hoja de estilo, datos de estilo para especificar cómo debe visualizarse, y también aplicaciones embebidas para así permitir interacción.

Las páginas web son escritas en un lenguaje de marcado que provee la capacidad de manejar e insertar hiperenlaces, generalmente HTML.

Respecto a la estructura de las páginas web, algunos organismos, en especial el World Wide Web Consortium, suelen establecer directivas con la intención de normalizar el diseño, y para así facilitar y simplificar la visualización e interpretación del contenido.

Una página web es en esencia una tarjeta de presentación digital, ya sea para empresas, organizaciones, o personas, así como una manera de comunicar ideas, pensamientos, conocimientos, informaciones o teorías. Así mismo, la nueva tendencia orienta a que las páginas web no sean sólo atractivas para los internautas, sino también optimizadas (preparadas), para los buscadores a través del código fuente. Forzar esta doble función puede, sin embargo, crear conflictos respecto de la calidad del contenido.

Unidad 2

> Marco legal

U2

Delitos informáticos

Desde hace unos años se viene observando un fuerte aumento en el uso de las tecnologías de la información y comunicación (TICs) en el mundo y, particularmente en la República Argentina, lo cual tiene como característica principal la afectación en todos los ámbitos de la actuación de los seres humanos y de las infraestructuras críticas (Estado, salud, comunicaciones, transporte, etc.).

En este crecimiento, se suma la fácil accesibilidad en el alcance de la tecnología, y por consiguiente ante la necesidad de que las personas se comuniquen, aumenta la tendencia al uso de herramientas tecnológicas, como correos electrónicos, redes sociales, etc., lo que a su vez refleja un mayor incremento en el manejo de internet en la vida cotidiana.

La utilización de internet, presenta entre otras características, la de ofrecer a una indeterminada cantidad de personas el anonimato para realizar infinidad de tareas.

Es así, que la "gran red de comunicación interconectada", pone al alcance de los usuarios innumerables instrumentos; sólo que algunas personas los utilizan en forma indebida, fraudulenta o con fines no convencionales que perturban la paz social, es decir, en contra del buen uso del resto de los usuarios.

Con el desembarco de la informática en la vida de las personas, el derecho tuvo que evolucionar para regular y proteger la información y los dispositivos.

En cuanto a la informática como objeto de estudio, es a través del ***derecho informático***, donde se aplican las reglas jurídicas con los problemas vinculados con la tecnología o la informática.

Hoy existe un área relacionada con el derecho penal, que consiste en el estudio de aquellas conductas donde la informática y la tecnología de la información, desempeñan un papel fundamental como medio para la comisión de un ilícito.

En la actualidad, el espectro de las acciones ilícitas se va acrecentando, poniéndose de manifiesto en la comisión de diferentes delitos que son cometidos por medios informáticos: ej. fraudes, obtención no autorizada de datos, pornografía infantil con la producción y su distribución, grooming, etc.

Estos tipos de ilícitos son los denominados: **delitos informáticos, delitos cibernéticos o cibercrímenes.**

Definición

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático.

Los también conocidos Ciberdelitos, como lo señala Téllez, son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas atípicas, anti jurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras; la manipulación de datos de entrada (sustraer datos), manipulación de programas (modificar programas del sistema o insertar nuevos programas o rutinas), manipulación de los datos de salida (fijación de un objeto al funcionamiento de sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a otras).

2. Manipulación de datos de entrada; como objetivo cuando se altera directamente los datos de una información computarizada. Como instrumento cuando se usan las computadoras como medio de falsificación de documentos.

3. Daños o modificaciones de programas o datos computarizados; entran tres formas de delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por sabotaje).

La criminalidad informática incluye una amplia variedad de delitos informáticos. El fenómeno se puede analizar en dos grupos:

1. Informática como objeto del delito: esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo (cracking es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad) y el DDNS (Denegación de servicio de nombres de dominio).

2. Informática como medio del delito: dentro de este grupo se encuentra la falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

Algunos ejemplos de delitos informáticos

Sabotaje informático

Implica que el *delincuente* recupere o busca destruir el centro de cómputos en sí (las máquinas) o los programas o informaciones almacenados en los ordenadores. Se presenta como uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito político.

Piratería informática

La piratería informática consiste en la violación ilegal del derecho de autor. Existen dos modalidades:

1. El hurto de tiempo de máquina.

2. La apropiación o hurto de software y datos: en este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio.

Cajeros automáticos y tarjetas de crédito

Conductas mediante las cuales se logra retirar dinero del cajero automático, utilizando una tarjeta magnética robada, o los números de la clave para el acceso a la cuenta con fondos.

El caso Chalmskinn

Se procede cuando se accede a ordenadores industriales centrales de la red para el uso específico de malgastar fondos para interrumpir los accesos a telefonía móvil.

Robo de identidad

Luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su información sensible. Encuadra como delito de estafa. Si el actuar del sujeto activo comporta dar a conocer datos personales ajenos contenidos en base de datos a las que por su empleo tiene acceso, entonces por expreso mandato legal la figura aplicable es la de revelación de secreto profesional.

Phreaking

Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando la cuenta ajena. Resulta ser una modalidad primitiva de hacking.

Regulación por países en el mundo

Convenio sobre cibercriminalidad

El Convenio sobre ciberdelincuencia, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Estados Unidos, Japón, Chile, Costa Rica y Filipinas.

El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, y entró en vigor el 1 de julio de 2004.

El 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre el delito cibernético entró en vigor. Los estados que han ratificado el Protocolo Adicional son

necesarios para penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como de las amenazas racistas y xenófobas e insultos.

El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.

2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.

3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Los siguientes delitos están definidos por el Convenio en los artículos 1 al 10:5 acceso ilícito, interceptación ilícita, ataque a la integridad de datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, los delitos relacionados con la pornografía infantil y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.

El Convenio fue firmado por Canadá, Japón, Estados Unidos y Sudáfrica, el 23 de noviembre de 2001 (la firma se llevó a cabo en Budapest, Hungría). Se han previsto nuevas

adhesiones por parte de otros Estados no europeos tal como México, El Salvador, Argentina, Costa Rica, Uruguay y Chile.

Argentina

La ley vigente

En Argentina sancionó el 4 de junio de 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Definiciones vinculadas a la informática

En el nuevo ordenamiento se establece que el término ***documento*** comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

Delitos contra menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

***Artículo 128**: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produzca, financie, ofrezca, comercialice, publique, facilite, divulgue o distribuya, 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 dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior 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.

Protección de la privacidad

***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 153 bis**: 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.

***Artículo 155:** Será reprimido con multa de 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 de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

***Artículo 157:** 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.*

***Artículo 157 bis:** 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 otra 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.

Delitos contra la propiedad

***Artículo 173 inciso 16:** (Incurre en el delito de defraudación)...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 183 del Código Penal:** (Incurre en el delito de daño)...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.*

***Artículo 184 del Código Penal:** (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes):*

***Inciso 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;

Inciso 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.*

Delitos contra las comunicaciones

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.*

Delitos contra la administración de justicia

Artículo 255: *Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.*

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500).

Delito sobre los Sistemas Informáticos

El 15 de noviembre de 2012, la Fiscalía General de la CABA dictó la Resolución 501/12, a través de la cual, creó como prueba piloto por el término de un año, el Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas, que actúa con competencia única en toda la Ciudad Autónoma de Buenos Aires, con el fin de investigar los delitos informáticos propiamente dichos, y aquellos que se cometen a través de internet que por su complejidad en la investigación o su dificultad en individualizar a los autores, merecen un tratamiento especializado. Existen diferentes delitos informáticos en donde es objeto el sistema informático, tales como Delito de Daño: La ley 26388 incorpora como segundo párrafo del art. 183 CP “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."

Delito agravado

La ley 26.388 agrega dos nuevas agravantes al art. 184 CP: 5) "ejecutarlo en archivos, registros, bibliotecas, 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".

Delitos informáticos vigentes en la legislación argentina

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 Código Penal)
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1 Código Penal)
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art.

153, párrafo 2 Código Penal)

- Acceso a un sistema o dato informático (art. 153 bis Código Penal)
- Publicación de una comunicación electrónica (art. 155 Código Penal)
- Acceso a un banco de datos personales (art. 157 bis, párrafo 1 Código Penal)
- Revelación de información registrada en un banco de datos personales (art. 157 bis, párrafo 2 Código Penal)
- Inserción de datos falsos en un archivo de datos personales (art. 157 bis, párrafo 2 Código Penal)
- Fraude informático (art. 173, inciso 16 Código Penal)
- Daño o sabotaje informático (art. 183 y 184, incisos 5 y 6 Código Penal)
- Ciberacoso a un menor y/o Grooming (art. 131 Código Penal)

¿Cuáles son los delitos informáticos más frecuentes?

En el código penal argentino hay al menos 45 tipos penales que pueden configurarse de forma directa a través de dispositivos informáticos. Los delitos más frecuentes en nuestro país son:

- Amenazas simples
- Amenazas coactivas
- Discriminación
- Xenofobia
- Fraude informático
- Extorsión
- Calumnias e injurias
- Incitación al odio
- Grooming o corrupción de menores en grado de tentativa
- Violación de correspondencia digital
- Incitación a la violencia
- Instigación a cometer delitos
- Apología del delito
- Violencia de género
- Delitos contra el orden público
- Pornografía infantil
- Acoso u hostigamiento (solamente en Ciudad de Bs As es considerado una contravención)
- Instigación al suicidio
- Usurpación de títulos y honores
- Ejercicio ilegal de la medicina
- Daño informático
- Acceso indebido a medios informáticos

- Delitos contra el orden democrático
- Violación a la propiedad intelectual

Pero también existen conductas dolosas aún no tipificadas en nuestro ordenamiento penal. El equipo de la AALCC viene trabajando desde el 2013 junto con diferentes diputados nacionales para que estas conductas que producen tanto daño a las víctimas, se transformen en delitos y los autores puedan ser juzgados y sancionados.

- Porno venganza
- Publicación ilegitima de imágenes íntimas
- Acopio de pornografía infantil
- Usurpación de identidad digital
- Ciberbullyng / acoso informático
- Ley integral sobre prueba informática
- Hostigamiento digital
- Cyberquating
- Mettataging
- Typosquatting

Pero esto no es todo, el avance de la tecnología lleva a que delincuentes comunes y crimen organizado utilice herramientas informáticas e internet como base necesaria para cometer diferentes delitos y/o perfeccionarlos:

- Secuestros virtuales
- Venta de productos provenientes de robos, hurtos, etc.
- Venta de estupefacientes, armas y/o productos ilegales
- Inteligencia criminal para cometer robos, secuestros, delitos contra la integridad mediante a la infiltración en redes sociales
- Comunicaciones entre delincuentes a través de plataformas de redes sociales, emails, aplicaciones encriptadas, etc.

Delitos informáticos propios e impropios

Los delitos informáticos pueden definirse como:

"La comisión de verdaderos actos ilícitos en los que se tengan a las computadoras como instrumento o fin".

"Se trata de 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".

"Delitos informáticos" es una denominación amplia que, al menos, puede diferenciarse entre propios e impropios, donde los primeros son aquellos que se pueden cometer sólo por medio de las TICs, y los segundos, delitos "clásicos" en los que las TICs son sólo un nuevo medio comisivo.

Migliorisi califica los delitos informáticos en dos tipos; los denominados propiamente "in- formáticos", que son aquellos que nunca podrían existir sin la informática y/o internet, tales como el hacking, el phishing ,el spamming, los hoax, las infecciones informáticas provocadas mediante virus o troyanos (programas espías) entre otros y los denominados "delitos configurados a través de internet" que son aquellos delitos históricamente tipificados en el Código Penal, pero que a través de la tecnología encuentran una nueva forma de realizarse, como por ejemplo, las diferentes variantes de delitos sexuales: pedofilia, pornografía infantil y corrupción de menores.

La informática como objeto y como medio del delito

La criminalidad informática incluye una amplia variedad de delitos informáticos. El fenómeno se puede analizar en dos grupos:

1. **Informática como objeto del delito**: esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo (cracking es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad) y el DDNS (Denegación de servicio de nombres de dominio).

2. **Informática como medio del delito**: dentro de este grupo se encuentra la falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

Hackers, crackers y nuevos perfiles de delincuentes asociados a las nuevas tecnologías.

Podemos clasificarlos en dos tipos, según los objetivos buscados. Por un lado estarían los hackers, o lo que es lo mismo, aquellos intrusos que acceden a los equipos de otros usuarios con la sola intención de demostrar sus habilidades; generalmente su objetivo no es dañar los sistemas informáticos, sino simplemente burlar los sistemas de seguridad de otros usuarios. Uno de los más famosos fue Dadee Murphy, apodado Zero Cool, quien en 1988 provocó la caída de 1.500 ordenadores en Wall Streeet y a quien las autoridades norteamericanas prohibieron tocar un sólo teclado hasta que cumpliera 18 años.

También existen otros cuya finalidad es la de apropiarse de información de terceros para su posterior difusión (como sería el caso Wikileaks), para hacer reivindicaciones sociales (como se autojustifica Anonymous) o como parte de la ciberguerra que se libra en la Red entre potencias rivales.

Por otra parte y de forma opuesta a los anteriores, están los crackers, que se introducen de forma ilegítima en los equipos con el fin, no sólo de acceder a la información, sino también con la intención de destruirla o de alterarla.

Estas actividades de ciberdelincuencia, tanto la del hacker como la del cracker, son consideradas delitos informáticos dado que suponen una intromisión ilegítima en sistemas y ordenadores ajenos.

Lugar del hecho real y virtual

El lugar del hecho

Es el espacio físico en donde se ha desarrollado un hecho probablemente delictivo. También denominado como escena del crimen, escena del hecho, escenario del delito, siendo más recomendable citarlo como lugar de los hechos.

El lugar del hallazgo

Es el espacio físico en donde se tienen a la vista o donde se encuentra por primera vez el material sensible relacionado con un hecho probablemente delictivo, sin que en dicho lugar se haya realizado la conducta penada o el delito. Generalmente este es el lugar, donde

en actos delictivos, se encuentra el cuerpo de la víctima o cuerpo del delito, y donde se inicia la investigación.

Lugar de enlace

Es el lugar o espacio físico en donde se identifican indicios que permiten establecer la relación entre el lugar de los hechos y el lugar del hallazgo.

El hábitat, son los lugares físicos donde pudo haber estado el sospechoso en alguna fase de los hechos o momentos cercanos al acto delictivo (antes o después). Por lo antes expuesto se puede decir que lo obrante en el lugar del hecho debe ser visto de dos maneras, o sea la interacción de sujeto-objeto y la inversa:

a. La primera es dinámica, es la acción del autor sobre el lugar, allí buscaremos el rastro, prueba o indicio que pudo haber dejado.

b. La segunda es pasiva (objeto-sujeto), es decir, aquellos elementos de la escena del crimen y sus alrededores que queden sobre el autor, o lo que pueda haberle transferido el lugar del hecho.

El lugar de los hechos o la escena del delito va a ser el punto de partida de toda investigación; sin embargo, ésta como recurso de investigación no tiene valor permanente y se deteriora con rapidez; por lo que debe ser tratada urgentemente para que quede protegida contra alteraciones y destrucción, antes y durante la búsqueda de indicios, y así proporcionar la información necesaria para orientar correctamente los esfuerzos en la investigación.

El lugar del hecho

Conceptos básicos

1. El lugar del hecho es el espacio físico en el que se ha producido un acontecimiento susceptible de una investigación científica criminal con el propósito de establecer su naturaleza y quiénes intervinieron.

2. Puede estar integrado por uno o varios espacios físicos interrelacionados por los actos del acontecimiento investigado.

3. Se caracteriza por la presencia de elementos, rastros y/o indicios que puedan develar las circunstancias o características de lo allí ocurrido.

4. Se denomina ESCENA DEL CRIMEN cuando la naturaleza, circunstancias y características del acontecimiento permitan sospechar la comisión de un delito.

5. Siempre será considerado potencial ESCENA DEL CRIMEN hasta que se determine lo contrario.

6. Verificada la existencia de la escena corresponde inmediatamente su preservación para garantizar la intangibilidad de los elementos, rastros o indicios que puedan existir y para evitar cualquier pérdida, alteración o contaminación.

Lugar del hecho virtual

Cuando se produce un delito informático existen dos escenas del crimen, una la del hecho real, correspondiente al lugar físico donde se encuentra el individuo operando las TIC, para cometer el delito. Y por otro lado el lugar del hecho virtual que sería el espacio de información dentro de las redes, por donde circulan las sentencias utilizadas para cometer dicho delito.

Características de la evidencia digital

La evidencia digital posee las siguientes características:

1. Volátil

2. Anónima

3. Duplicable

4. Alterable y modificable

5. Eliminable

Estas características hacen de la evidencia digital un constante desafío para la identificación y el análisis, que exige al grupo de seguridad y auditoría la capacitación tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito.

Antes de realizar el proceso de análisis forense el equipo de seguridad o auditoría debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense:

▸ Esterilidad de los medios informáticos de trabajo

Los medios informáticos utilizados deben estar libres de variaciones magnéticas, ópticas (láser) o similares, esto significa que los medios deben ser nuevos para evitar que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática.

▸ Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas, para esto, se debe utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia.

▸ Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

El equipo de seguridad debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona del grupo de auditoría pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al equipo, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

▸ Mantenimiento de la cadena de custodia de las evidencias digitales

La custodia de todos los elementos allegados al caso y en poder del equipo de seguridad, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha

efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada protección de las pruebas a su cargo.

Definición de Informática forense

"Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que ésta sea legalmente aceptable"

Convenio sobre la ciberdelincuencia de Budapest

También denominado Convenio de Cibercriminalidad, ha establecido la adopción por los Estados Parte de "medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c. La difusión o transmisión de pornografía infantil por medio de un sistema informático;

d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos

Ley 27.411

Ley 27.411

Aprobación de la Convención de Budapest sobre Ciberdelito B.O. del 15/12/2017

Convenio sobre Ciberdelito. Aprobación.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTÍCULO 1°.- Apruébese el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, que consta de CUARENTA Y OCHO (48) artículos cuya copia auténtica de su traducción al español así como de su versión en idioma inglés, como ANEXO I, forma parte de la presente.

ARTÍCULO 2°.- Al depositarse el instrumento de adhesión deberán efectuarse las siguientes reservas:

a) La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal.

b) La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388.

c) La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL).

d) La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional.

e) La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.

ARTÍCULO 3°.- Comuníquese al Poder Ejecutivo nacional.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, EL 22 NOV 2017

— REGISTRADO BAJO EL N 27411 —

MARTA G. MICHETTI. — EMILIO MONZO. — Eugenio Inchausti. — Juan P. Tunessi.

Convenio sobre cibercriminalidad (Budapest, 23.XI. 2001)

Los Estados miembros del Consejo de Europa y los otros Estados firmantes,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados parte en el Convenio;

Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios suscitados por el incremento, la convergencia y la mundialización permanente de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes;

Reconociendo la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información;

Estimando que una lucha bien organizada contra la cibercriminalidad requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz;

Convencidos de que el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable;

Persuadidos de la necesidad de garantizar un equilibrio adecuado entre los intereses de la acción represiva y el respeto de los derechos fundamentales del hombre, como los garantizados en el Convenio para la protección de los derechos del hombre y de las

libertades fundamentales del Consejo de Europa (1950), en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada;

Conscientes, igualmente, de la protección de los datos personales, como la que confiere, por ejemplo, el Convenio de 1981 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal;

Considerando el Convenio de Naciones Unidas relativo a los derechos del niño y el Convenio de la Organización Internacional del Trabajo sobre la prohibición de las peores formas de trabajo infantil (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre la cooperación en materia penal, así como otros tratados similares suscritos entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio tiene por objeto completarlos con el fin de hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recogida de pruebas electrónicas de una infracción penal;

Felicitándose por las recientes iniciativas destinadas a mejorar la comprensión y la cooperación internacional para la lucha contra la criminalidad en el ciberespacio y, en particular, las acciones organizadas por las Naciones Unidas, la OCDE, la Unión europea y el G8;

Recordando la Recomendación N. (85) 10 sobre la aplicación práctica del Convenio europeo de ayuda mutua judicial en materia penal respecto a las comisiones rogatorias para la vigilancia de las telecomunicaciones, la Recomendación N. (88) 2 sobre medidas dirigidas a combatir la piratería en el ámbito de los derechos de autor y de los derechos afines, la Recomendación N. (87) 15 dirigida a regular la utilización de datos de carácter personal en el sector de la policía, la Recomendación N. (95) 4 sobre la protección de los datos de carácter personal en el sector de los servicios de telecomunicación, teniendo en cuenta, en particular, los servicios telefónicos y la Recomendación N. (89) 9 sobre la delincuencia relacionada con el ordenador, que indica a los legisladores nacionales los principios directores para definir ciertas infracciones informáticas, así como la Recomendación N. (95) 13 relativa a los problemas de procedimiento penal vinculados a las tecnologías de la información;

Vista la Resolución N. 1, adoptada por los Ministros europeos de Justicia, en su 21ª Conferencia (Praga, junio 1997), que recomienda al Comité de Ministros mantener las actividades organizadas por el Comité europeo para los problemas penales (CDPC) relativas

a la cibercriminalidad a fin de acercar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de infracciones informáticas, así como la Resolución N. 3, adoptada en la 23ª Conferencia de Ministros europeos de Justicia (Londres, junio 2000), que anima a las partes negociadoras a persistir en sus esfuerzos al objeto de encontrar soluciones adecuadas, que permitan al mayor número posible de Estados ser partes en el Convenio y reconoce la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional, que tenga en cuenta las específicas exigencias de la lucha contra la cibercriminalidad;

Tomando igualmente en cuenta el Plan de acción adoptado por los Jefes de Estado y de gobierno del Consejo de Europa, con ocasión de su Décima Cumbre (Estrasburgo, 10-11 octubre 1997) a fin de buscar respuestas comunes al desarrollo de las nuevas tecnologías de la información, fundadas sobre las normas y los valores del Consejo de Europa; Han convenido lo siguiente:

Capítulo I. Terminología

Artículo 1. Definiciones

A los efectos del presente Convenio, la expresión:

a. «sistema informático» designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b. «datos informáticos» designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c. «prestador de servicio»1 designa:

1. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

2. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d. «datos de tráfico» 2 designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II. Medidas que deben ser adoptadas a nivel nacional

Sección 1. Derecho penal material.

Título 1. Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Artículo 2. Acceso ilícito

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3. Interceptación ilícita

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos--en transmisiones no públicas-- en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Los Estados podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4. Atentados contra la integridad de los datos

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Los Estados podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5. Atentados contra la integridad del sistema

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6. Abuso de equipos e instrumentos técnicos

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición

1. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

2. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Los Estados podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a) (2).

Título 2. Infracciones informáticas

Artículo 7. Falsedad informática

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Los Estados podrán reservarse el derecho a exigir la concurrencia de

un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8. Estafa informática

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a. la introducción, alteración, borrado o supresión de datos informáticos,

b. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

***Título 3. Infracciones relativas al contenido**.*

Artículo 9. Infracciones relativas a la pornografía infantil

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;

c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;

d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

a. un menor adoptando un comportamiento sexualmente explícito;

b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;

c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito;

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Los Estados podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Los Estados podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado

por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5. Otras formas de responsabilidad y sanción

Artículo 11. Tentativa y complicidad

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

3. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12. Responsabilidad de las personas jurídicas

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en: a. un poder de representación de la persona jurídica; b. una autorización para tomar decisiones en nombre de la persona jurídica; c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, los Estados firmantes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Artículo 13. Sanciones y medidas

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.

2. Los Estados velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2. Derecho procesal Título 1. Disposiciones comunes

Artículo 14. Ámbito de aplicación de las medidas de derecho procesal

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, los Estados podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;

b. a cualquier otra infracción penal cometida a través de un sistema informático; y

c. a la recogida de pruebas electrónicas de cualquier infracción penal.

3.

a. Los Estados podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

I. es utilizado en beneficio de un grupo de usuarios cerrado, y

II. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo

que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artículo 15. Condiciones y garantías.

1. Los Estados velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido

2. en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad. 2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Los Estados examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

Título 2. Conservación inmediata de datos informáticos almacenados

Artículo 16. Conservación inmediata de datos informáticos almacenados

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Los Estados adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de

conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 17. Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 3. Mandato de comunicación

Artículo 18. Mandato de comunicación

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios;

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la 13 facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio;

c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Título 4. Registro y decomiso de datos informáticos almacenados

Artículo 19. Registro y decomiso de datos informáticos almacenados

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y

b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático;

b. realizar y conservar una copia de esos datos informáticos;

c. preservar la integridad de los datos informáticos almacenados pertinentes; y

d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado.

4. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 5. Recogida en tiempo real de datos informáticos

Artículo 20. Recogida en tiempo real de datos de tráfico

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

I. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

II. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 21. Interceptación de datos relativos al contenido

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

I. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

II. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Sección 3. Competencia

Artículo 22. Competencia

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción 16 penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

a. en su territorio;

b. a bordo de una nave que ondee pabellón de ese Estado;

c. a bordo de una aeronave inmatriculada en ese Estado;

d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Los Estados podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Los Estados firmantes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

Capítulo III. Cooperación internacional

Sección 1. Principios generales

Título 1. Principios generales relativos a la cooperación internacional

Artículo 23. Principios generales relativos a la cooperación internacional

Los Estados firmantes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Título 2. Principios relativos a la extradición

Artículo 24. Extradición

1.

a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE n 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Los Estados se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Los Estados que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto –la demanda del Estado requirente a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado. 18

7.

a. Los Estados firmantes deberán comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito del instrumento de ratificación, aceptación,

aprobación o adhesión, el nombre y la dirección de las autoridades responsables del envío y de la recepción de una demanda de extradición o de arresto provisional, en caso de ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por los Estados. Los Estados deberán garantizar la exactitud de los datos obrantes en el registro.

Título 3. Principios generales relativos a la colaboración

Artículo 25. Principios generales relativos a la colaboración

1. Los Estados firmantes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Los Estados firmantes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción en relación a la que se solicita la colaboración se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

Artículo 26. Información espontánea

1. Los Estados podrán, dentro de los límites de su derecho interno y en ausencia de demanda previa, comunicar a otro Estado las informaciones obtenidas en el marco de investigaciones que puedan ayudar a la parte destinataria a iniciar o a concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el presente Convenio, o a que dicha parte presente una demanda de las previstas en el presente capítulo.

2. Antes de comunicar dicha información, ese Estado podrá solicitar que la información sea tratada de forma confidencial o que sea utilizada sólo en ciertas circunstancias. Si el Estado destinatario no pudiera acatar las condiciones impuestas, deberá informar al otro Estado, quien habrá de decidir si proporciona o no la información. Una vez aceptadas estas condiciones por el Estado destinatario, éste quedará obligado a su cumplimiento.

Título 4. Procedimientos relativos a las demandas de asistencia en ausencia de acuerdo internacional aplicable

Artículo 27. Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2.

a. Los Estados designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Los Estados, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las partes. Los Estados deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público u otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos. Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9.

a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente parágrafo podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Los Estados podrán informar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

Artículo 28. Confidencialidad y restricciones de uso

1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

3. Si el Estado requirente no pudiera satisfacer alguna de las circunstancias establecidas en el apartado 2 del presente artículo, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

Sección 2. Disposiciones específicas

Título 1. Cooperación en materia de medidas cautelares

Artículo 29. Conservación inmediata datos informáticos almacenados

1. Los Estados firmantes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

a. la identificación de la autoridad que solicita la conservación;

b. la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;

c. los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;

d. todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;

e. justificación de la necesidad de conservación; y

f. la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.

4. Si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los artículos 2 a 11 del presente Convenio, podrá negarse a la demanda de conservación, al amparo del presente artículo, si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación.

5. Al margen de lo anterior, una demanda de conservación únicamente podrá ser denegada: a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o; b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público u otro interés esencial.

6. Cuando el Estado requerido considere que la simple conservación no será suficiente para garantizar la disponibilidad futura de los datos informáticos o que ésta podría comprometer la confidencialidad de la investigación o podría hacerla fracasar de otro modo, deberá informar inmediatamente al Estado requirente, quien decidirá la conveniencia de dar curso a la demanda.

7. Todas las conservaciones realizadas al amparo de una demanda de las previstas en el párrafo 1 serán válidas por un periodo máximo de 60 días, para permitir, en ese plazo de tiempo, al Estado requirente formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos. Después de la recepción de la demanda, los datos informáticos deberán mantenerse hasta que ésta se resuelva.

Artículo 30. Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada: a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o; b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público u otro interés esencial.

Título 2. Asistencia en relación a los poderes de investigación

Artículo 31. Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.

2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo. 3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o

b. cuando los instrumentos, convenios o legislación referida en el párrafo 2 prevean una cooperación rápida.

Artículo 32. Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Artículo 33. Asistencia para la recogida en tiempo real de datos de tráfico

1. Los Estados podrán acordar colaborar en la recogida, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. Dicha colaboración se someterá a las condiciones y procedimientos previstos en el derecho interno, salvo que alguna de las partes se acoja a la reserva prevista en el párrafo 2.

2. Los Estados deberán acordar colaborar respecto a aquellas infracciones penales para las cuales la recogida en tiempo real de datos de tráfico se encuentra prevista en su derecho interno en situaciones análogas.

Artículo 34. Asistencia en materia de interceptación de datos relativos al contenido

Los Estados podrán acordar colaborar, en la medida en que se encuentre previsto por tratados o leyes internas, en la recogida y registro, en tiempo real, de datos relativos al contenido de concretas comunicaciones realizadas a través de sistemas informáticos.

Título 3. Red 24/7

Artículo 35. Red 24/7

1. Los Estados designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

a. aportación de consejos técnicos;

b. conservación de datos según lo dispuesto en los artículos 29 y 30; y

c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2.

a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Los Estados dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Capítulo IV. Cláusulas finales

Artículo 36. Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio está sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación deberán ser entregados al Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes transcurridos tres meses desde que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, presten su consentimiento a vincularse al Convenio, conforme a lo dispuesto en los párrafos 1 y 2.

4. Para todos los Estados que hayan prestado su consentimiento a vincularse al Convenio, éste entrará en vigor el primer día del mes transcurridos tres meses desde que hayan expresado su consentimiento, conforme a lo dispuesto en los párrafos 1 y 2.

Artículo 37. Adhesión al Convenio

1. Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a los Estados firmantes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del mismo a adherirse al Convenio. Esta decisión deberá tomarse mediante la mayoría prevista en el artículo 20.d del Estatuto del Consejo de 26 Europa y el asentimiento unánime de los Estados firmantes que tengan derecho a formar parte del Comité de Ministros.

2. Para todos aquellos Estados que se adhieran al Convenio conforme a lo previsto en el párrafo precedente, el Convenio entrará en vigor el primer día del mes transcurridos tres meses después del depósito del instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38. Aplicación territorial

1. Los Estados podrán, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, designar el territorio al que resultará aplicable el presente Convenio.

2. Los Estados podrán, en cualquier momento, a través de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a otros territorios diversos a los designados en la declaración. En tal caso, el Convenio entrará en vigor en dichos territorios el primer día del mes transcurridos tres meses desde la recepción de la declaración por el Secretario General.

3. Toda declaración realizada al amparo de los párrafos precedentes podrá ser retirada, en lo que concierne al territorio designado en la citada declaración, a través de una notificación dirigida al Secretario General del Consejo de Europa. El retracto surtirá efecto el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 39. Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales existentes entre las partes, y comprende las disposiciones: del Convenio Europeo de extradición abierto a la firma el 13 de diciembre de 1957 en París (STE n 24) - del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE n 30). - del Protocolo Adicional del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE n 99).

2. Si dos o más Estados han concluido un acuerdo o un tratado relativo a la materia objeto de este Convenio o si han establecido de otro modo la relación entre ellos, o si lo hacen en el futuro, dispondrán igualmente de la facultad de aplicar el citado acuerdo o de establecer sus relaciones con base en el mismo, en lugar del presente Convenio. Siempre que los Estados hayan establecido sus relaciones concernientes a la materia objeto del presente Convenio de forma 27 diversa, éstas deberán llevarse a cabo de forma compatible con los objetivos y principios del Convenio.

3. Lo dispuesto en el presente Convenio no afectará a otros derechos, restricciones, obligaciones y responsabilidades de los Estados.

Artículo 40. Declaraciones

A través de una declaración escrita dirigida al Secretario General del Consejo de Europa, los Estados podrán, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, declarar que se reservan el derecho a exigir,

llegado el caso, uno o varios elementos suplementarios de los dispuestos en los artículos 2, 3, 6 del párrafo 1 (b), 7, 9 párrafo 3 y 27 del párrafo 9 (e).

Artículo 41. Cláusula federal

1. Un Estado federal podrá reservarse el derecho de desempeñar sus obligaciones, en los términos previstos en el capítulo II del presente Convenio, en la medida en que éstas sean compatibles con los principios que presiden las relaciones entre el gobierno central y los Estados federados u otros territorios análogos, siempre que se garantice la cooperación en los términos previstos en el capítulo III.

2. Un Estado federal no podrá hacer uso de la reserva adoptada según lo dispuesto en el párrafo 1 para excluir o disminuir de forma substancial las obligaciones contraídas en virtud del capítulo II. En todo caso, el Estado federal deberá dotarse de los medios necesarios para dar cumplimiento a las medidas previstas en el citado capítulo.

3. En todo lo que concierne a las disposiciones de este Convenio cuya aplicación dimana de la competencia de cada uno de los Estados federados u otras entidades territoriales análogas, que no están, en virtud del sistema constitucional de la federación, obligados a adoptar medidas legislativas, el gobierno central pondrá, con la aprobación de éstos, en conocimiento de las autoridades competentes de los Estados federados la necesidad de adoptar las citadas medidas animándolos a que las ejecuten.

Artículo 42. Reservas

Los Estados podrán, a través de una notificación escrita dirigida al Secretario del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o de adhesión, declarar que invocan la reserva o reservas previstas en el art. 4, párrafo 2, artículo 6, párrafo 3, artículo 9, párrafo 4, artículo 10, párrafo 3, artículo 11, párrafo 3, artículo 14, párrafo 3, artículo 22, párrafo 2, artículo 29, párrafo 4 y en el artículo 41, párrafo 1. No podrá realizarse ninguna otra reserva diversa a las indicadas.

Artículo 43. Mantenimiento y retirada de las reservas

1. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42 podrá retirarla total o parcialmente notificando tal extremo al Secretario General. La retirada se hará efectiva en la fecha de recepción por el Secretario General de la notificación. Si en la notificación se hiciera constar que la reserva deberá tener efecto en una determinada fecha, ello se hará efectivo siempre que sea posterior a la recepción por el Secretario General de la notificación.

2. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42, podrá retirarla total o parcialmente siempre que lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a los Estados, que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre la posibilidad de su retirada.

Artículo 44. Enmiendas

1. Las enmiendas al presente Convenio podrán ser propuestas por los Estados firmantes, y deberán ser comunicadas al Secretario General del Consejo de Europa, a los Estados miembros del Consejo de Europa, a los Estados no miembros del Consejo de Europa que hayan tomado parte en la elaboración del Convenio así como a los Estados que se hayan adherido o que hayan sido invitados a adherirse conforme a lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por uno de los Estados deberán ser comunicadas al Comité europeo para los problemas criminales (CDPC), quien deberá informar al Comité de Ministros sobre las mismas.

3. El Comité de Ministros examinará la enmienda propuesta y el informe del Comité europeo para los problemas criminales (CDPC) y, después de consultar con los Estados no miembros y partes del Convenio, podrá adoptar la enmienda.

4. El texto de la enmienda adoptado por el Comité de Ministros, conforme a lo dispuesto en el párrafo 3 del presente artículo, deberá comunicarse a los Estados para su aceptación.

5. Las enmiendas adoptadas conforme al párrafo 3 del presente artículo entrarán en vigor el trigésimo día después del que los Estados hayan informado al Secretario General de su aceptación.

Artículo 45. Reglamento de controversia

1. El Comité europeo para los problemas criminales (CDPC) está obligado a informar de la interpretación y aplicación del presente Convenio.

2. En caso de diferencias entre los Estados sobre la interpretación o aplicación del presente Convenio, los Estados intentarán adoptar un reglamento de diferencia a través de la negociación o de cualquier otro medio pacífico, con el compromiso de someter la controversia al Comité europeo para los problemas criminales, a un tribunal arbitral que tomará las decisiones que los Estados le sometan, o a la Corte internacional de justicia, a partir de un acuerdo adoptado por los Estados en litigio.

Artículo 46. Reuniones de los Estados

1. Los Estados deberán reunirse periódicamente a fin de facilitar:

a. el uso y el efectivo cumplimiento del presente Convenio, la identificación de los problemas en esta materia, así como el efecto de las declaraciones o reservas formuladas conforme al presente Convenio;

b. el intercambio de información sobre novedades jurídicas, políticas o técnicas observadas en la criminalidad informática y recogida de pruebas electrónicas;

c. el examen sobre la posible reforma del Convenio.

2. El Comité europeo para los problemas criminales (CDPC) deberá estar al corriente de las reuniones llevadas a cabo al amparo del párrafo 1.

3. El Comité europeo para los problemas criminales (CDPC) deberá facilitar las reuniones previstas en el párrafo 1 y adoptar las medidas necesarias para ayudar a los Estados a completar o modificar el Convenio. No más tarde de tres años a contar desde la entrada en vigor del presente Convenio, el Comité europeo para los problemas criminales (CDPC) procederá, en cooperación con los Estados, a un examen conjunto de las disposiciones de la Convención y propondrá, en su caso, las modificaciones pertinentes.

4. Salvo que el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 deberán ser soportados por los Estados del modo que ellos mismos determinen.

5. Los Estados estarán asistidos por el Secretario del Consejo de Europa en lo relativo al ejercicio de las funciones derivadas del presente artículo.

Artículo 47. Denuncia

1. Los Estados podrán, en cualquier momento, denunciar el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. La denuncia entrará en vigor el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General. Artículo 48. Notificación 30 El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan tomado parte en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse:

a. cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c. la fecha de entrada en vigor del presente Convenio según lo dispuesto en los artículos 36 y 37;

d. cualquier declaración hecha por mor de los artículos 40 y 41 o cualquier reserva formulada en virtud del artículo 42;

e. cualquier acto, notificación o comunicación referida al presente Convenio.

En vista de lo cual, los abajo firmantes, debidamente autorizados al efecto, han firmado el presente Convenio. Hecho en [Budapest], el [23 noviembre 2001], en francés y en inglés, ambos textos con el mismo valor, y en un solo ejemplar que será depositado en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse.

Ley 26.388

Ley 26.388

Sancionada: Junio 4 de 2008 Promulgada de Hecho: Junio 24 de 2008 Código Penal

Modificación.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. Sancionan con fuerza de Ley:

***Artículo 1**. Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes:*

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

***Artículo 2**. Sustitúyase el artículo 128 del Código Penal, por el siguiente:*

***Artículo 128**: Será reprimido con prisión de seis (6) meses a cuatro (4) 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 dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior 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.

***Artículo 3**. Sustitúyase el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad"*

***Artículo 4.** Sustitúyase el artículo 153 del Código Penal, por el siguiente:*

***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 5.** Incorporase como artículo 153 bis del Código Penal, el siguiente:*

***Artículo 153 bis**: 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.*

***Artículo 6.** Sustitúyase el artículo 155 del Código Penal, por el siguiente:*

***Artículo 155:** Será reprimido con multa de 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 de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 7. *Sustitúyase el artículo 157 del Código Penal, por el siguiente:*

Artículo 157: *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.*

Artículo 8. *Sustitúyase el artículo 157 bis del Código Penal, por el siguiente:*

Artículo 157 bis*: 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.

Artículo 9. *Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 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 10. *Incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente: 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.*

Artículo 11*. Sustitúyase el artículo 184 del Código Penal, por el siguiente:*

Artículo 184: *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.

***Artículo 12**. Sustitúyase el artículo 197 del Código Penal, por el siguiente:*

***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.*

***Artículo 13**. Sustitúyase el artículo 255 del Código Penal, por el siguiente:*

***Artículo 255**: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.*

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

***Artículo 14**. Deróguense el artículo 78 bis y el inciso 1 del artículo 117 bis del Código Penal.*

***Artículo 15**. Comuníquese al Poder Ejecutivo.*

Delitos informáticos

¿Qué establece la ley?

La ley incorpora al Código Penal delitos cometidos por medios informáticos.

¿Qué es un documento para el código penal?

Es la representación de actos o hechos sin importar el soporte utilizado para almacenarlo o transmitirlo. Pueden ser figuras o imágenes que se ven como: dibujos, pinturas, fotografías, retratos, películas cinematográficas, etc. Estas representaciones pueden estar en un soporte físico en uno informático.

Delitos contra la integridad sexual. Pornografía infantil.

¿Qué conductas sanciona el código penal?

El código penal sanciona las siguientes conductas:

- Producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir por cualquier medio, cualquier representación de una persona menor de 18 años dedicado a actividades sexuales explícitas o de sus partes genitales.

- Tener representaciones de personas menores de edad para distribuirlas o comercializarlas.

- Organizar espectáculos en vivo de representaciones sexuales explícitas en las que participan personas menores de edad.

- Facilitar el acceso a espectáculos pornográficos o dar material pornográfico a personas menores de 14 años.

Violación de secretos y de la privacidad

¿Qué conductas sanciona el código penal?

El Código Penal sanciona las siguientes conductas:

- Abrir o acceder indebidamente una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido.

- Apoderarse indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado aunque no esté cerrado.

- Suprimir o desviar de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

- Interceptar o captar comunicaciones electrónicas o telecomunicaciones de carácter privado o de acceso restringido.

La pena se agrava si el autor comunica o pública el contenido de la carta, escrito, despacho o comunicación electrónica y esto causa perjuicio. Si el hecho lo comete un funcionario público que abusa de sus funciones, sufre además, inhabilitación.

Acceso a sistema informático

¿Qué conductas sanciona el código penal?

El Código Penal sanciona el acceso por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema informático de acceso restringido. La pena se agrava 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.

Acceso a banco de datos

¿Qué conductas sanciona el código penal?

El Código penal sanciona las siguientes conductas:

- Acceder ilegítimamente a un banco de datos personales.

- Proporcionar o revelar información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a guardar por ley.

- Insertar o hacer insertar datos en un archivo de datos personales.

Si el autor es funcionario público, sufre además pena de inhabilitación especial.

Publicación de una comunicación electrónica

¿Qué conductas sanciona el código penal?

El Código Penal sanciona la publicación indebida de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad y esto cause perjuicio a otros. Está exento de responsabilidad penal el que actúa con el propósito de proteger un interés público.

Fraude informático

¿Qué conducta sanciona el código penal?

El Código Penal sanciona la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Daño informático

¿Qué conductas sanciona el código penal?

El Código Penal sanciona las siguientes conductas:

- Alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos.
- Vender, distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños.

La pena se agrava si el autor:

- Realiza el hecho para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
- Realiza el hecho para producir infección o contagio en aves u otros animales domésticos;
- Emplea substancias venenosas o corrosivas;

- Comete el delito en despoblado y en banda;

- Realiza el hecho 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;

- Realiza el hecho 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.

Documento electrónico y digital

La definición que ofrece el Diccionario de la Real Academia Española:

«Documento. (Del lat. documentum). m. Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos. || 2. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo. || 3. desus. Instrucción que se da a alguien en cualquier materia, y particularmente aviso y consejo para apartarle de obrar mal. || ~ auténtico. m. Der. El que está autorizado o legalizado. || ~ privado. m. Der. El que, autorizado por las partes interesadas, pero no por funcionario competente, prueba contra quien lo escribe o sus herederos. || ~ público. m. Der. El que, autorizado por funcionario para ello competente, acredita los hechos que refiere y su fecha.»

Esta definición, no nos ayuda mucho, ya que hace un excesivo hincapié en los aspectos etimológicos, históricos, jurídicos y administrativos y olvida por completo otros muchos, entre ellos el sentido que el término tiene para una ciencia a la que ha dado nombre y origen y de la que el documento es el principal objeto de estudio: la ciencia documental.

En el terreno de la ciencia documental, la mayor parte de autores coinciden en que un documento es, esencialmente, información, la materialización de un mensaje o el soporte de una información. Un documento, no es ni más ni menos, que un soporte para transferir información. Para la ciencia de la documentación, el documento es a la vez medio y mensaje de información y conocimiento. De esta manera, el documento se caracteriza por una triple dimensión: el soporte físico o material, el mensaje informativo y la posibilidad de transmisión o difusión de este conocimiento.

Clasificación tradicional de los tipos de documentos

Esta triple dimensión que caracteriza al documento ha servido, a su vez, para establecer una tipología de los documentos en la que los estudiosos del campo de la documentación coinciden, más o menos, y que se puede establecer de la siguiente forma:

Según el soporte material

- papel: (libros, revistas, folletos, etc.)
- material químico (películas)
- material magnético (cintas de vídeo, disquete de ordenador, casetes, etc.)
- soportes ópticos (CD-ROM, DVD, video-discos, etc.)
- material plástico (microformas: microfichas)

Según el mensaje informativo

- por la forma de expresión del contenido
    - Documentos textuales
    - Documentos no textuales:
    - Gráficos (mapas, planos, etc.)
    - Sonoros (cintas, discos, etc.)
    - Iconográficos (cuadros, diapositivas, fotografías, etc.)
    - Audiovisuales (películas, vídeos, etc.)
    - Informáticos (legibles por ordenador)
    - Tridimensionales o plásticos (esculturas, etc.)
    - Compuestos o multimedia (cuando el documento combina varios de los anteriores)
- por el nivel y rigor del contenido
    - científicos
    - técnico-profesionales
    - culturales-divulgativos
    - sociales
- por la transformación del contenido
    - primarios: originales
    - secundarios: hacen referencia a los primarios (bibliografías, catálogos, índices, sumarios, etc.)

- terciarios: tienen estructura formal de secundarios, pero contenido primario (diccionarios, enciclopedias, léxicos, tesauros, etc.)
- mixtos: tienen elementos primarios y secundarios (bibliografías comentadas, resúmenes o abstracts, etc.)

Según la posibilidad de transmisión o difusión:

- social
  - públicos
  - reservados
  - inéditos
  - personales
- temporal
  - periódicos
  - no periódicos

En este tipo de clasificaciones tradicionales, no encontramos por ningún lado términos como electrónico, digital, hipertextual, virtual, etc. Será necesario, pues, ampliar esta tipología para dar cabida a los nuevos tipos de documentos surgidos gracias a la revolución digital, la tecnología hipertextual y la aparición de la Web y la red Internet como depósito universal de informaciones y conocimientos donde es posible acceder a documentos de muy diverso signo y condición.

Documento electrónico - documento impreso

El término electrónico empezó a cobrar importancia en documentación cuando proliferaron los medios audiovisuales y los bibliotecarios y documentalistas se dieron de bruces con el problema de catalogar una serie de documentos especiales, sin saber en un principio si atender a la clase de soporte (librario o no librario) o a la clase de signo en que se expresaba el contenido (textual o no textual). Un casete, por ejemplo, podía contener únicamente música, pero también podía ser un audiolibro, e incluso, muchas veces llegaba el casete empaquetado junto al libro impreso formando una unidad.

La proliferación de los medios audiovisuales junto a los tradicionales medios impresos, hizo que se estableciera una oposición clara entre documentos electrónicos y documentos no electrónicos, puesto que era importante conocer si los documentos

necesitaban la mediación de algún aparato electrónico auxiliar o, si por el contrario, eran legibles de manera directa sin la mediación de éste.

Un documento electrónico difiere de un documento impreso en el material que lo conforma. Tablas de cera o arcilla, papiro, pergamino y papel han abierto paso a los discos y cintas magnéticas (cassette, cinta de vídeo, disquete, disco duro de un ordenador, tarjetas de memoria, etc.) y a los discos ópticos (CD-ROM, DVD, etc.) que se imprimen y leen mediante láser sin que exista un contacto directo con el soporte. Ambos, documento impreso y documento electrónico, pueden contener el mismo texto, lo que cambia es el soporte.

Un documento electrónico es aquel contenido en un soporte electrónico que, para su visualización requiere una pantalla textual, una pantalla gráfica, y/o unos dispositivos de emisión de audio, vídeo, etc.; según el tipo de información que contenga. En algunos casos también se precisa la mediación de un ordenador (cuando la información está digitalizada), en otros no (si se trata de información analógica).

Documento digital/documento analógico

A menudo se identifica un documento electrónico con un documento digital, sin embargo, no son la misma cosa. Los términos electrónico y digital no son sinónimos, aunque suelen utilizarse como tales en los pares biblioteca electrónica/biblioteca digital, libro electrónico/libro digital, edición electrónica/edición digital, información electrónica/información digital, documento electrónico/documento digital, etc.

Todo documento digital es un documento electrónico pero no ocurre lo mismo al revés, no todo documento electrónico es un documento digital. Un documento electrónico puede ser bien analógico, bien digital. Documentos electrónicos son, por ejemplo, una cinta de casete o una cinta de vídeo, que precisan de un dispositivo electrónico para su lectura, pero no son digitales. Lo que distingue un medio electrónico de un medio digital es, por una parte, la forma en que está codificada la información y, por otra, la necesaria mediación de un ordenador para descodificar esta información. En el caso de un documento digital, la información está codificada en bits, y para leer, visualizar o grabar la información se precisa de un dispositivo que transmita o grabe información codificada en bits. Al representarse digitalmente, los datos de entrada son convertidos en dígitos (0,1) inteligibles para la máquina y no para los sentidos humanos; y a la salida, otro dispositivo los convertirá en señales analógicas, inteligibles para los sentidos humanos. Un documento digital es, pues, aquel que contiene la información codificada en bits.

De esta manera, las distintas morfologías de texto, imagen y sonido se pitagorizan y se integran en una: la forma digital, ceros y unos. En realidad, los bits no son inmateriales, sino que se trata de electrones que se mueven en los pequeños chips de silicio de la memoria de los ordenadores y otros dispositivos. Los archivos grabados en los chips de memoria del ordenador u otros dispositivos sí ocupan lugar y prueba de ellos es que

frecuentemente se saturan los discos duros de nuestros ordenadores, los CDs y DVDs grabables, las tarjetas de memoria de nuestras cámaras fotográficas digitales, etc.

La dicotomía, pues, no sólo se establece entre documento impreso y documento electrónico, sino también y dentro de los propios documentos electrónicos, entre documento digital y documento analógico.

Firma electrónica

La firma electrónica es un concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta y da por validado el contenido de un mensaje electrónico a través de cualquier medio electrónico que sea legítimo y permitido.

Ejemplos:

- Usando una firma biométrica.
- Firmando con un lápiz electrónico al usar una tarjeta de crédito o débito en un comercio.
- Marcando una casilla en una computadora, a máquina, o aplicada con el ratón o incluso con el dedo del usuario en una pantalla táctil.
- Usando una firma digital.
- Usando un sistema que obligue a establecer usuario y contraseña.
- Usando una tarjeta de coordenadas.

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes: Código secreto o de ingreso: es la necesidad de una combinación determinada de números o letras, que son solo conocidas por el dueño del documento, o lo que todos usamos por ejemplo en los cajeros automáticos, el conocido PIN (Personal Identificación Number); también, métodos basados en la biometría: se permite el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento; la forma de identificación en este caso consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos.

Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz). En el perfeccionamiento del cifrado de mensajes, llegamos a lo que se conoce como criptografía, que consiste en un sistema de codificación de un texto con claves de carácter confidencial y procesos matemáticos complejos, de manera que para el tercero resulta incomprensible el documento si desconoce la clave decodificadora, que permite visualizar el documento en su forma original; de ahí es que surgen dos tipos de criptografía:

De clave secreta o simétrica: las partes en los dos procesos de cifrado y descifrado comparten una clave común previamente acordada; debe ser conocida solamente por ambas partes, para evitar que un tercero ajeno a la operación pueda descifrar el mensaje transmitido y de esa forma hacer caer toda la seguridad del sistema.

Por ese motivo surgió el sistema de clave asimétrica o de doble clave, clave pública y clave privada. Este sistema fue creado por investigadores de la Universidad de Stanford en 1976, y tal como lo indica su nombre, el sistema posee dos claves: una de ellas solo es conocida por el autor del documento y la otra puede ser conocida por cualquier persona; si bien esas dos claves se encuentran relacionadas matemáticamente mediante un algoritmo, no es posible por medio de la clave pública, conocer la clave privada, por lo menos en los estándares tecnológicos actuales.

Una firma electrónica crea un historial de auditoría que incluye la verificación de quién envía el documento firmado y un sello con la fecha y hora.

Según la Ley 59/2003 en España, la firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Según la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de fecha 13 de diciembre de 1999, se establece un marco comunitario para la firma electrónica, que dice: la firma electrónica son los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación.

Tipos

- Simple: No identifica y genera disputas.
- Avanzada: Conocida como firma biométrica, es la firma electrónica que permite identificar al firmante y detectar cualquier cambio en la integridad de un documento es decir, vincula firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Cualificada: Utiliza un dispositivo cualificado de Firma Electrónica.

Regulación en Argentina

La firma digital es legislada en la ley 25506 de la República Argentina. Fue sancionada en noviembre de 2001 y promulgada en el mismo año.

La ley distingue a la firma digital de la firma electrónica, siendo la primera la de mayor peso jurídico: se establece que la firma digital es equivalente a la firma manuscrita. Esa equivalencia se exceptúa en los siguientes casos:

1. a las disposiciones por causa de muerte;

2. a los actos jurídicos del derecho de familia;

3. a los actos personalismos en general;

4. a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o por acuerdo de partes.

(Estas exclusiones han sido derogadas primero por el l Decreto de Necesidad y Urgencia N° 27/2018 modificó la regulación de la Ley N° 25.056 de Firma Digital y luego por el Decreto Reglamentario N° 182/2019)

A diferencia de la firma electrónica, la firma digital es posible gracias al uso de certificados digitales. Esos certificados contienen datos que identifican al titular de una firma. Los certificados digitales son entregados por Certificadores registrados y autorizados para tal actividad, y pueden ser empresas, registros, u organismos públicos especialmente autorizados.

Son los certificados digitales los que permiten a un tercero establecer la autenticidad de un firmante y detectar la alteración de documentos electrónicos firmados digitalmente.

Por otro lado, la exigencia de establecer la autenticidad del firmante en la firma electrónica recae en el mismo firmante, dado que carece de los requisitos legales para ser considerada firma digital. En cambio, la autenticidad del firmante en la firma digital se presume, salvo prueba en contrario.

Firma digital

La firma digital de un documento se obtiene tras una operación en tres pasos:

1. Se aplica al documento un algoritmo matemático que crear una huella digital llamada hash. Este hash es un número que identifica de forma inequívoca el documento.

2. El hash se encripta usando la llave privada del firmante.

3. El hash encriptado y la pública del firmante se combinan en una firma digital que se agrega al documento.

Para verificar la autenticidad del documento el receptor debe tener un programa que soporte firmas digitales. El programa usa la llave pública para desencriptar la clave hash. Luego calcula un nuevo hash para el documento. De este modo puede comparar el hash calculado con el hash desencriptado; si coinciden, el documento no ha sido modificado.

Asimismo el programa valida que la llave pública usada en la firma pertenece al nombre que lo ha firmado.

Delitos contra la integridad sexual

Sin perjuicio de las circunstancias específicas que podrían rodear a los niños, niñas y adolescentes, como la pobreza, las redes de tráfico infantil y los conflictos armados, las que podrían aumentar su vulnerabilidad, ellos son los seres más indefensos de la población, el sector más vulnerable de la sociedad, «tienen poco o ningún poder para protegerse o asegurar su sustento, y poca influencia en lo mucho que es vital para su bienestar».

En el ámbito sexual, abusar de un niño, niña o adolescente, resulta más fácil que abusar de un adulto. Los explotadores sexuales aprovechan su docilidad para hacerlo, ya que su capacidad para defenderse es menor. La motivación de los explotadores, frecuentemente radica, en querer obtener un sentimiento de poder sexual o económico, buscar experiencias nuevas o en la sensación de impunidad que proporciona el anonimato.

La violencia sexual en los niños, niñas y adolescentes, «ocurre en todos los niveles socioeconómicos, razas, etnias y culturas, en todos los niveles de educación y en todas las religionesr». La inmensa mayoría de los casos, suelen ocurrir dentro del círculo doméstico o familiar, aunque a veces adquieren una dimensión internacional. Éstos están expuestos a mayor riesgo de abuso a través de la producción de pornografía, en su casa y su familia. Por lo general conocen a la(s) persona(s) que ejerce(n) el abuso sexual como un padre, miembro de la familia, tutor u otra persona que está cerca de la misma.

Prostitución infantil

Por prostitución infantil se entiende “la utilización de un niño en actividades sexuales a cambio de remuneración o de cualquier otra retribución”.

Humanium, una ONG internacional de apadrinamiento de niños comprometida a acabar con las violaciones de los Derechos del Niño en el mundo, define a la prostitución infantil como “el uso de niños en actividades sexuales a cambio de una remuneración o cualquier otro tipo de retribución (por ejemplo regalos, comida o vestimenta). Esta actividad se inscribe también bajo el término explotación sexual”. Los niños, niñas y adolescentes

“trabajan en las calles o en establecimientos como burdeles, discotecas, centros de masajes, bares, hoteles o restaurantes”.

Pornografía infantil

Por pornografía infantil se entiende: “toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales”

Ésta puede clasificarse en: “blanda o dura” de acuerdo se representen niños, niñas o adolescentes desnudos, posando provocativamente o actúen en escenas de sexo explícito; “infantil real o virtual” si se utilizan personas reales o dibujos animados participando en actividades sexuales y por último en “técnica o sesudo infantil”, que se logra alterando imágenes por ordenador, enmascarando las presentaciones pornográficas de adultos para que simulen ser infantes

Mayormente, las imágenes pornográficas distribuidas en internet, son producidas fuera de línea, pero también se puede organizar el abuso para ser visto en tiempo real, lo que es facilitado mediante las cámaras web, o aquéllas integradas a los teléfonos móviles y las transmisiones de video. “Un público recibirá un aviso en el momento en que debe conectarse a ver a un niño ser abusado sexualmente. Los miembros del público pueden estar en cualquier lugar en el mundo. Pueden pagar dinero o intercambiar con la persona directamente responsable del abuso de los niños”.

Pedofilia

En un artículo publicado por UNICEF, se refiere que los explotadores de niños, niñas o adolescentes no tienen un perfil uniforme y que si bien no se pueden categorizar simplemente, una clase de explotadores son los denominados pedófilos; adultos que sienten una atracción sexual por los niños y están listos para cualquier cosa para satisfacer sus necesidades.

“La Pedofilia reúne todo aquello que se trata de relaciones sexuales entre adultos y niños. Puede ser heterosexual, homosexual, o mixto. Implica hombres y mujeres de todas las edades”

No se conforma únicamente con el acto sexual, sino que también “puede conformarse simplemente con imágenes o fantasías eróticas”.

Tipos de pedófilos

En función de su comportamiento, los pedófilos pueden clasificarse en tres categorías:

- Los perversos: pedófilos que habitualmente tienen un discurso perfectamente estructurado o proselitismo para justificar su conducta, presentado como educativo y saludable para el niño.

- Los psicópatas: un pervertido sádico capaz de ocasionar daño físico grave e incluso el asesinato.

- Los señores de todo el mundo: son hombres (y también mujeres) que están tentados por la relación sexual con un niño, impulsados por el deseo de originalidad, por unos pocos dólares en una tierra lejana permitiendo todo libertinaje. Después regresan a las 'sociedades civilizadas' dónde vuelven para continuar su vida cotidiana, en su mayoría como ciudadanos inocentes.

Grooming

Grooming, es un vocablo de habla inglesa vinculado al verbo "groom". Llevado el concepto a personas menores de edad, se refiere a "preparar a un niño o a una niña a través de comunicaciones informáticas para abusar sexualmente de ellos" Puede definirse como "el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad, a través de Internet, con el fin último de obtener concesiones de índole sexual" o la "seducción de los menores de edad con fines sexuales..." , mediante medios digitales o de telecomunicaciones: internet, whatsapp o twitter y su finalidad es cometer un delito contra la integridad sexual del menor .

La persona que lleva a cabo esta acción se denomina groomer y es quien intenta desplegar toda una estrategia para hacerse amigo del menor, logrando que ceda sus inhibiciones y adquiriendo su confianza hasta obtener el acoso sexual o el abuso en el peor de los casos.

En Argentina el Grooming es un delito penal, descripto en la Ley 26.904 sancionada el 13 de noviembre de 2013.

Ley N° 26.904. Ley de 'Grooming' en Argentina

Artículo 1º. *Incorporase como artículo 131 del Código Penal el siguiente:*

'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.'

Artículo 2°. *Comuníquese al Poder Ejecutivo.*

Ley 27.436

Ley 27.436

Modificación.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Artículo 1°. *Sustitúyase el artículo 128 del Código Penal por el siguiente:*

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.

Artículo 2°. *Comuníquese al Poder Ejecutivo nacional.*

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, EL 21 MAR 2018

Trata de personas

Es una violación de los Derechos Humanos y una forma de conducta criminal que afecta a personas de todo el mundo.

En el año 2000, la Asamblea General de la Naciones Unidas adoptó el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, especialmente Mujeres y Niños. Este Protocolo proporciona la primera definición internacionalmente acordada de trata de personas y muestra el compromiso de comunidad internacional para contrarrestar este delito. Requiere que los Estados Partes promulguen leyes nacionales que penalicen la trata de personas; prevengan y combatan la trata de personas; protejan y asistan a las víctimas de la trata; cooperen con otros estados para cumplir estos objetivos.

El artículo 3. a del Protocolo proporciona la única definición internacional aceptada de trata de personas.

Artículo. 3 a: ... *"La trata de personas significa el reclutamiento, transporte, transferencia, albergue o recepción de personas, mediante la amenaza o el uso de la fuerza u otras formas de coerción, secuestro, fraude, engaño, abuso de poder o de una posición de vulnerabilidad o de dar o recibir pagos o beneficios para lograr el consentimiento de una persona que tiene control sobre otra persona, con fines de explotación. La explotación incluirá, como mínimo la explotación de la prostitución, de otros u otras formas de explotación sexual, trabajo o servicio forzado, esclavitud o prácticas similares a la esclavitud, la servidumbre o la extracción de órganos humanos"*

Ley 26.842. Trata de personas

Ley 26.842

CÓDIGO PENAL - CÓDIGO PROCESAL PENAL

Trata de personas y asistencia a sus víctimas. Prevención y sanción. Código Penal y

Código Procesal Penal. Modificación.

Sanc. 19/12/2012 ; Promul. 26/12/2012 ; Publ. 27/12/2012

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

***Artículo 1°.** Sustitúyese el artículo 2° de la ley 26.364 por el siguiente:*

Artículo 2 *Se entiende por trata de personas el ofrecimiento, la captación, el traslado, la recepción o acogida de personas con fines de explotación, ya sea dentro del territorio nacional, como desde o hacia otros países.*

A los fines de esta ley se entiende por explotación la configuración de cual- quiera de los siguientes supuestos, sin perjuicio de que constituyan delitos autónomos res-pecto del delito de trata de personas:

a. Cuando se redujere o mantuviere a una persona en condición de esclavitud o servidumbre, bajo cualquier modalidad;

b. Cuando se obligare a una persona a realizar trabajos o servicios forzados;

c. Cuando se promoviere, facilitare o comercializare la prostitución ajena o cualquier otra forma de oferta de servicios sexuales ajenos;

d. Cuando se promoviere, facilitare o comercializare la pornografía infantil o la realización de cualquier tipo de representación o espectáculo con dicho contenido

e. Cuando se forzare a una persona al matrimonio o a cualquier tipo de unión de hecho;

f. Cuando se promoviere, facilitare o comercializare la extracción forzosa o ilegitima de órganos, fluidos o tejidos humanos

El consentimiento dado por la víctima de la trata y explotación de personas no constituirá en ningún caso causal de eximición de responsabilidad penal, civil o administrativa de los autores, partícipes, cooperadores o instigadores

Artículo 2°*. Deróganse los artículos 3° y 4° de la ley 26.364.*

Artículo 3°*. Sustitúyese la denominación del Título II de la ley 26.364 por la siguiente:*

Título II. Garantías mínimas para el ejercicio de los derechos de las víctimas.

Artículo 4°*. Sustitúyese el artículo 6° de la ley 26.364 por el siguiente:*

Artículo 6°. *El Estado nacional garantiza a la víctima de los delitos de trata o explotación de personas los siguientes derechos, con prescindencia de su condición de denunciante o querellante en el proceso penal correspondiente y hasta el logro efectivo de las reparaciones pertinentes:*

a. Recibir información sobre los derechos que le asisten en su idioma y en forma accesible a su edad y madurez, de modo tal que se asegure el pleno acceso y ejercicio de los derechos económicos, sociales y culturales que le correspondan;

b. Recibir asistencia psicológica y médica gratuitas, con el fin de garantizar su reinserción social;

c. Recibir alojamiento apropiado, manutención, alimentación suficiente y elementos de higiene personal;

d. Recibir capacitación laboral y ayuda en la búsqueda de empleo;

e. Recibir asesoramiento legal integral y patrocinio jurídico gratuito en sede judicial y administrativa, en todas las instancias;

f. Recibir protección eficaz frente a toda posible represalia contra su persona o su familia, quedando expeditos a tal efecto todos los remedios procesales disponibles a tal fin. En su caso, podrá solicitar su incorporación al Programa Nacional de Protección de Testigos en las condiciones previstas por la ley 25.764;

g. Permanecer en el país, si así lo decidiere, recibiendo la documentación necesaria a tal fin. En caso de corresponder, será informada de la posibilidad de formalizar una petición de refugio en los términos de la ley 26.165;

h. Retornar a su lugar de origen cuando así lo solicitare. En los casos de víctima residente en el país que, como consecuencia del delito padecido, quisiera emigrar, se le garantizará la posibilidad de hacerlo;

i. Prestar testimonio en condiciones especiales de protección y cuidado;

j. Ser informada del estado de las actuaciones, de las medidas adoptadas y de la evolución del proceso;

k. Ser oída en todas las etapas del proceso;

l. A la protección de su identidad e intimidad;

m. A la incorporación o reinserción en el sistema educativo;

n. En caso de tratarse de víctima menor de edad, además de los derechos precedentemente enunciados, se garantizara que los procedimientos reconozcan sus necesidades especiales que implican la condición de ser un sujeto en pleno desarrollo de la personalidad. Las medidas de protección no podrán restringir sus derechos y garantías, ni implicar privación de su libertad. Se procurara la reincorporación a su núcleo familiar o al lugar que mejor proveyere para su protección y desarrollo.

***Artículo 5°**. Sustitúyese el artículo 9 de la ley 26.364 por el siguiente:*

***Artículo 9°:** Cuando la víctima del delito de trata o explotación de personas en el exterior del país tenga ciudadanía argentina, será obligación de los representantes diplomáticos del Estado Nacional efectuar ante las autoridades locales las presentaciones*

necesarias para garantizar su seguridad y acompañarla en todas las gestiones que deba realizar ante las autoridades del país extranjero. Así mismo dichos representantes arbitraran los medios necesarios para posibilitar de ser requerida por la víctima, su repatriación.

***Artículo 6**. Sustitúyese el Título IV de la ley 26.364 por el siguiente:*

***Título IV.**Consejo Federal para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas.*

***Artículo 7**. Sustitúyese el artículo 18 de la ley 26.364 por el siguiente:*

***Artículo 18:** Créase el Consejo Federal para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas, que funcionará dentro del ámbito de la Jefatura de Gabinete de Ministros, con el fin de constituir un ámbito permanente de acción y coordinación institucional para el seguimiento de todos los temas vinculados a esta ley, que contará con autonomía funcional, y que estará integrado del siguiente modo:*

1. Un representante del Ministerio de Justicia y Derechos Humanos.

2. Un representante del Ministerio de Seguridad.

3. Un representante del Ministerio del Interior.

4. Un representante del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto.

5. Un representante del Ministerio de Desarrollo Social.

6. Un representante del Ministerio de Trabajo, Empleo y Seguridad Social.

7. Un representante de la Cámara de Diputados de la Nación, elegido a propuesta del pleno.

8. Un representante de la Cámara de Senadores de la Nación, elegido a propuesta del pleno.

9. Un representante del Poder Judicial de la Nación, a ser designado por la Corte Suprema de Justicia de la Nación.

10. Un representante por cada una de las provincias y por la Ciudad Autónoma de Buenos Aires.

11. Un representante del Ministerio Público Fiscal.

12. Un representante del Consejo Nacional de Niñez, Adolescencia y Familia.

13. Un representante del Consejo Nacional de las Mujeres.

14. Tres representantes de organizaciones no gubernamentales, las que serán incorporadas de acuerdo a lo establecido en el artículo 19 de la presente ley.

15. El Consejo Federal designará un coordinador a través del voto de las dos terceras partes de sus miembros, en los términos que establezca la reglamentación.

Artículo 8°. *Sustitúyese el artículo 19 de la ley 26.364 por el siguiente:*

Artículo 19: *Una vez constituido, el Consejo Federal para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas habilitará un registro en el que se inscribirán las organizaciones no gubernamentales de Derechos Humanos o con actividad específica en el tema, que acrediten personería jurídica vigente y una existencia no menor a tres (3) años.*

La reglamentación dispondrá el modo en que, de manera rotativa y por períodos iguales no superiores a un (1) año, las organizaciones inscriptas integrarán el Consejo Federal de acuerdo a lo establecido en el artículo anterior.

Artículo 9°. *Sustitúyese el artículo 20 de la ley 26.364 por el siguiente:*

Artículo 20*: El Consejo Federal para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas tiene las siguientes funciones:*

a. Diseñar la estrategia destinada a combatir la trata y explotación de personas, supervisando el cumplimiento y efectividad de las normas e instituciones vigentes;

b. Recomendar la elaboración y aprobación de normas vinculadas con el objeto de esta ley; y, en general, participar en el diseño de las políticas y medidas necesarias que aseguren la eficaz persecución de los delitos de trata y explotación de personas y la protección y asistencia a las víctimas;

c. Promover la adopción por parte de las diversas jurisdicciones de los estándares de actuación, protocolos y circuitos de intervención que aseguren la protección eficaz y el respeto a los derechos de las víctimas de los delitos de trata y explotación de personas;

d. Supervisar el cumplimiento de las funciones correspondientes al Comité Ejecutivo creado en el Título V de la presente ley;

e. Analizar y difundir periódicamente los datos estadísticos y los informes que eleve el Comité Ejecutivo a fin de controlar la eficacia de las políticas públicas del área solicitándole toda información necesaria para el cumplimiento de sus funciones;

f. Promover la realización de estudios e investigaciones sobre la problemática de la trata y explotación de personas, su publicación y difusión periódicas;

g. Diseñar y publicar una Guía de Servicios en coordinación y actualización permanente con las distintas jurisdicciones, que brinde información sobre los programas y los servicios de asistencia directa de las víctimas de los delitos de trata y explotación de personas;

h. Promover la cooperación entre Estados y la adopción de medidas de carácter bilateral y multilateral, destinadas a controlar, prevenir y erradicar la trata y explotación de personas. Esta cooperación tendrá como fin fortalecer los medios bilaterales, multilaterales, locales y regionales para prevenir el delito de trata de personas, posibilitar el enjuiciamiento y castigo de sus autores y asistir a las víctimas;

i. Impulsar el proceso de revisión de los instrumentos internacionales y regionales que haya suscripto la República, con el fin de fortalecer la cooperación internacional en la materia;

j. Redactar y elevar un informe anual de su gestión, el que deberá ser aprobado por el Congreso de la Nación. Una vez aprobado, dicho informe será girado al Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, para su presentación ante los organismos internacionales y regionales con competencia en el tema;

k. Aprobar el plan de acción bianual que elabore el Comité Ejecutivo;

l. Dictar su reglamento interno, el que será aprobado con el voto de los dos tercios de sus miembros.

La Defensoría del Pueblo de la Nación será el organismo de control externo del cumplimiento de los planes y programas decididos por el Consejo Federal.

***Artículo 10**. Incorpórase como Título V de la ley 26.364 (*), el siguiente:*

(*) Texto según fe de erratas publ. 31/12/2012; texto anterior "26.634".

Título V

Comité Ejecutivo para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas.

***Artículo 11**. Incorpórase como artículo 21 de la ley 26.364, el siguiente:*

Artículo 21: Créase el Comité Ejecutivo para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas que funcionará en el ámbito de la Jefatura de Gabinete de Ministros, con autonomía funcional, y que estará integrado del siguiente modo:

1. Un representante del Ministerio de Seguridad.

2. Un representante del Ministerio de Justicia y Derechos Humanos.

3. Un representante del Ministerio de Desarrollo Social.

4. Un representante del Ministerio de Trabajo, Empleo y Seguridad Social.

Artículo 12. *Incorpórase como artículo 22 de la ley 26.364, el siguiente:*

Artículo 22: *El Comité Ejecutivo para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas tiene a su cargo la ejecución de un Programa Nacional para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas, que consistirá en el desarrollo de las siguientes tareas:*

a. Diseñar estándares de actuación, protocolos y circuitos de intervención que contribuyan a prevenir y combatir los delitos de trata y explotación, y a proteger y asistir a las víctimas de tales delitos y sus familias;

b. Desarrollar acciones eficaces orientadas a aumentar la capacidad de detección, persecución y desarticulación de las redes de trata y explotación;

c. Asegurar a las víctimas el respeto y ejercicio pleno de sus derechos y garantías, proporcionándoles la orientación técnica para el acceso a servicios de atención integral gratuita (médica, psicológica, social, jurídica, entre otros);

d. Generar actividades que coadyuven en la capacitación y asistencia para la búsqueda y obtención de oportunidades laborales, juntamente con los organismos pertinentes;

e. Prever e impedir cualquier forma de revictimización de las víctimas de trata y explotación de personas y sus familias;

f. Llevar adelante un Registro Nacional de Datos vinculados con los delitos de trata y explotación de personas, como sistema permanente y eficaz de información y monitoreo cuantitativo y cualitativo. A tal fin se deberá relevar periódicamente toda la información que pueda ser útil para combatir estos delitos y asistir a sus víctimas. Se solicitará a los funcionarios policiales, judiciales y del Ministerio Público la remisión de los datos requeridos a los fines de su incorporación en el Registro;

g. Organizar actividades de difusión, concientización, capacitación y entrenamiento acerca de la problemática de los delitos de trata y explotación de personas, desde las directrices impuestas por el respeto a los derechos humanos, la perspectiva de género y las cuestiones específicas de la niñez y adolescencia;

h. Promover el conocimiento sobre la temática de los delitos de trata y explotación de personas y desarrollar materiales para la formación docente inicial y continua, desde

un enfoque de derechos humanos y desde una perspectiva de género, en coordinación con el Ministerio de Educación;

i. Impulsar la coordinación de los recursos públicos y privados disponibles para la prevención y asistencia a las víctimas, aportando o garantizando la vivienda indispensable para asistirlas conforme lo normado en la presente ley

j. Capacitar y especializar a los funcionarios públicos de todas las instituciones vinculadas a la protección y asistencia a las víctimas, así como a las fuerzas policiales, instituciones de seguridad y funcionarios encargados de la persecución penal y el juzgamiento de los casos de trata de personas con el fin de lograr la mayor profesionalización;

k. Coordinar con las instituciones, públicas o privadas, que brinden formación o capacitación de pilotos, azafatas y todo otro rol como tripulación de cabina de aeronaves o de medios de transporte terrestre, internacional o de cabotaje, un programa de entrenamiento obligatorio específicamente orientado a advertir entre los pasajeros posibles víctimas del delito de trata de personas

l. Coordinar con las provincias y la Ciudad Autónoma de Buenos Aires la implementación del Sistema Sincronizado de Denuncias sobre los Delitos de Trata y Explotación de Personas. Realizar en todo el territorio nacional una amplia y periódica campaña de publicidad del Sistema y el número para realizar denuncias.

El Comité Ejecutivo elaborará cada dos (2) años un plan de trabajo que deberá ser presentado ante el Consejo Federal para su aprobación. Deberá también elaborar y presentar anualmente ante el Consejo Federal informes sobre su actuación a los fines de que éste pueda ejercer sus facultades de supervisión. Estos informes serán públicos.

A los fines de hacer efectiva la ejecución del Programa, el Comité Ejecutivo coordinará su accionar con las provincias, la Ciudad Autónoma de Buenos Aires y organismos nacionales e internacionales.

***Artículo 13**. Incorpórase como Título VI de la ley 26.364 el siguiente:*

Título VI. Sistema Sincronizado de Denuncias sobre los delitos de Trata y Explotación de Personas

***Artículo 14**. Incorpórase como artículo 23 de la ley 26.364 el siguiente:*

***Artículo 23:** Créase en el ámbito del Ministerio Público Fiscal el Sistema Sincronizado de Denuncias sobre los Delitos de Trata y Explotación de Personas.*

***Artículo 15**. Incorpórase como artículo 24 de la ley 26.364 el siguiente:*

***Artículo 24**: A fin de implementar el Sistema mencionado en el artículo anterior, asígnasele el número telefónico ciento cuarenta y cinco (145), uniforme en todo el territorio nacional, que funcionará en forma permanente durante las veinticuatro horas del día a fin de receptar denuncias sobre los delitos de trata y explotación de personas. Las llamadas telefónicas entrantes serán sin cargo y podrán hacerse desde teléfonos públicos, semipúblicos, privados o celulares.*

Asimismo, se garantizará el soporte técnico para desarrollar e implementar el servicio de mensajes de texto o SMS (Short Message Service) al número indicado, para receptar las denuncias, los que serán sin cargo.

***Artículo 16**. Incorpórase como artículo 25 de la ley 26.364 el siguiente:*

***Artículo 25**: El Ministerio Público Fiscal conservará un archivo con los registros de las llamadas telefónicas y de los mensajes de texto o SMS (Short Message Service) identificados electrónicamente, los que serán mantenidos por un término no menor a diez (10) años, a fin de contar con una base de consulta de datos para facilitar la investigación de los delitos de trata y explotación de personas.*

***Artículo 17**. Incorpórase como artículo 26 de la ley 26.364 el siguiente:*

***Artículo 26:** Las denuncias podrán ser anónimas. En caso de que el denunciante se identifique, la identidad de esta persona será reservada, inclusive para las fuerzas de seguridad que intervengan.*

***Artículo 18**. Incorpórase como Título VII de la ley 26.364 el siguiente: Título VII. Disposiciones Finales.*

***Artículo 19**. Incorpórase como artículo 27 de la ley 26.364 el siguiente:*

***Artículo 27:** El Presupuesto General de la Nación incluirá anualmente las partidas necesarias para el cumplimiento de las disposiciones de la presente ley. Asimismo, los organismos creados por la presente ley se podrán financiar con recursos provenientes de acuerdos de cooperación internacional, donaciones o subsidios.*

Los decomisos aplicados en virtud de esta ley tendrán como destino específico un fondo de asistencia directa a las víctimas administrado por el Consejo Federal para la Lucha contra la Trata y Explotación de Personas y para la Protección y Asistencia a las Víctimas.

***Artículo 20**. Sustituyese el sexto párrafo del artículo 20 del Código Penal por el siguiente. En el caso de condena impuesta por alguno de los delitos previstos por los artículos 125, 125 bis, 127, 140, 142 bis, 145 bis, 145 ter y 170 de este Código, queda comprendido entre los bienes a decomisar la cosa mueble o inmueble donde se mantuviera a la víctima privada de su libelad u objeto de explotación. Los bienes decomisados con motivo*

de tales delitos, según los términos del presente artículo, y el producido de las multas que se impongan, serán afectados a programas de asistencia a la víctima.

***Artículo 21**. Sustitúyese el artículo 125 bis del Código Penal por el siguiente:*

***Artículo 125 bis**: El que promoviere o facilitare la prostitución de una persona será penado con prisión de cuatro (4) a seis (6) años de prisión, aunque mediare el consentimiento de la víctima.*

***Artículo 22**. Sustitúyese el artículo 126 del Código Penal por el siguiente:*

***Artículo 126:** En el caso del artículo anterior, la pena será de cinco (5) a diez (10) años de prisión, si concurriere alguna de las siguientes circunstancias:*

1. Mediare engaño, fraude, violencia, amenaza o cualquier otro medio de intimidación o coerción, abuso de autoridad o de una situación de vulnerabilidad, o concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre la víctima.

2. El autor fuere ascendiente, descendiente, cónyuge, afín en línea recta, colateral o conviviente, tutor, curador, autoridad o ministro de cualquier culto reconocido o no, o encargado de la educación o de la guarda de la víctima.

3. El autor fuere funcionario público o miembro de una fuerza de seguridad, policial o penitenciaria.

Cuando la víctima fuere menor de dieciocho (18) años la pena será de diez (10) a quince (15) años de prisión.

***Artículo 23**. Sustitúyese el artículo 127 del Código Penal por el siguiente:*

***Artículo 127:** Será reprimido con prisión de cuatro (4) a seis (6) años, el que explotare económicamente el ejercicio de la prostitución de una persona, aunque mediare el consentimiento de la víctima.*

La pena será de cinco (5) a diez (10) años de prisión, si concurriere alguna de las siguientes circunstancias:

1. Mediare engaño, fraude, violencia, amenaza o cualquier otro medio de intimidación o coerción, abuso de autoridad o de una situación de vulnerabilidad, o concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre la víctima.

2. El autor fuere ascendiente, descendiente, cónyuge, afín en línea recta, colateral o conviviente, tutor, curador, autoridad o ministro de cualquier culto reconocido o no, o encargado de la educación o de la guarda de la víctima.

3. El autor fuere funcionario público o miembro de una fuerza de seguridad, policial o penitenciaria.

Cuando la víctima fuere menor de dieciocho (18) años la pena será de diez (10) a quince (15) años de prisión.

***Artículo 24.** Sustitúyese el artículo 140 del Código Penal por el siguiente:*

Artículo 140: Serán reprimidos con reclusión o prisión de cuatro (4) a quince (15) años el que redujere a una persona a esclavitud o servidumbre, bajo cualquier modalidad, y el que la recibiere en tal condición para mantenerla en ella. En la misma pena incurrirá el que obligare a una persona a realizar trabajos o servicios forzados o a contraer matrimonio servil.

***Artículo 25**. Sustitúyese el artículo 145 bis del Código Penal por el siguiente:*

***Artículo 145 bis**: Será reprimido con prisión de cuatro (4) a ocho (8) años, el que ofreciere, captare, trasladare, recibiere o acogiere personas con fines de explotación, ya sea dentro del territorio nacional, como desde o hacia otros países, aunque mediare el consentimiento de la víctima.*

***Artículo 26**. Sustitúyese el artículo 145 ter del Código Penal por el siguiente:*

***Artículo 145 ter**: En los supuestos del artículo 145 bis la pena será de cinco (5) a diez (10) años de prisión, cuando:*

1. Mediare engaño, fraude, violencia, amenaza o cualquier otro medio de intimidación o coerción, abuso de autoridad o de una situación de vulnerabilidad, o concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre la víctima.

2. La víctima estuviere embarazada, o fuere mayor de setenta (70) años.

3. La víctima fuera una persona discapacitada, enferma o que no pueda valerse por sí misma.

4. Las víctimas fueren tres (3) o más.

5. En la comisión del delito participaren tres (3) o más personas.

6. El autor fuere ascendiente, descendiente, cónyuge, afín en línea recta, colateral o conviviente, tutor, curador, autoridad o ministro de cualquier culto reconocido o no, o encargado de la educación o de la guarda de la víctima.

7. El autor fuere funcionario público o miembro de una fuerza de seguridad policial o penitenciaria.

Cuando se lograra consumar la explotación de la víctima objeto del delito de trata de personas la pena será de ocho (8) a doce (12) años de prisión.

Cuando la víctima fuere menor de dieciocho (18) años la pena será de diez (10) a quince (15) años de prisión.

***Artículo 27**. Incorpórase como artículo 250 quáter del Código Procesal Penal el siguiente: **Artículo 250 quáter**: Siempre que fuere posible, las declaraciones de las víctimas de los delitos de trata y explotación de personas serán entrevistadas por un psicólogo designado por el Tribunal que ordene la medida, no pudiendo en ningún caso ser interrogadas en forma directa por las partes.*

Cuando se cuente con los recursos necesarios, las víctimas serán recibidas en una "Sala Gesell", disponiéndose la grabación de la entrevista en soporte audiovisual, cuando ello pueda evitar que se repita su celebración en sucesivas instancias judiciales. Se deberá notificar al imputado y a su defensa de la realización de dicho acto. En aquellos procesos en los que aún no exista un imputado identificado los actos serán desarrollados con control judicial, previa notificación al Defensor Público Oficial.

Las alternativas del acto podrán ser seguidas desde el exterior del recinto a través de vidrio espejado, micrófono, equipo de video o cualquier otro medio técnico con que se cuente. En ese caso, previo a la iniciación del acto, el Tribunal hará saber al profesional a cargo de la entrevista el interrogatorio propuesto por las partes, así como las inquietudes que surgieren durante el transcurso de la misma, las que serán canalizadas teniendo en cuenta las características del hecho y el estado emocional de la víctima.

Cuando se trate de actos de reconocimiento de lugares u objetos, la víctima será acompañada por el profesional que designe el Tribunal no pudiendo en ningún caso estar presente el imputado.

***Artículo 28.** Esta ley será reglamentada en un plazo máximo de noventa (90) días contados a partir de su promulgación.*

***Artículo 29**. El Poder Ejecutivo dictará el texto ordenado de la ley 26.364, de conformidad a lo previsto en la ley 20.004.*

***Artículo 30**. Comuníquese al Poder Ejecutivo nacional.*

Grooming

Se denomina así a la situación en que un adulto acosa sexualmente a un niño o niña mediante el uso de las TICs. Los perpetradores de este delito suelen generar un perfil falso

en una red social, sala de chat, foro, videojuego u otro, en 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,

El mecanismo del grooming consta de varias fases o etapas. Suele comenzar con un pedido de foto o video de índole sexual o erótica (pedido por el adulto, utilizando el perfil falso). Cuando consigue ese material, quien lo pide puede o bien desaparecer o bien chantajear a la víctima con hacer público esa información si no entrega nuevos videos o fotos o si no accede a un encuentro personal. Como se dijo anteriormente, las TICs son herramientas que brindan nuevos escenarios para problemáticas previamente existentes. Es decir, el abuso o acoso sexual a chicos y la pedofilia no surgen con internet y las redes sociales, ya que estas son problemáticas que anteceden la existencia de estos espacios. Lo que sí sucede es que se constituyen en instrumentos capaces de potenciar los distintos tipos de abuso.

En Argentina, el grooming es un delito penado por la ley n° 26.904 e incluido en el Código Penal. La penalización incluye prisión de 6 meses a 4 años a quien por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier tecnología de transmisión de datos, contacte a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Tipos de grooming

Hay dos tipos de grooming:

1. Sin fase previa de relación y generación de confianza el acosador logra tener fotos o videos sexuales de los chicos y chicas mediante la obtención de contraseñas o hackeo de cuentas. Con el material sexual o erótico en mano, extorsiona al chico o chica con mostrarlo si este no le entrega más material o accede a un encuentro personal. En este caso el material es obtenido a la fuerza, y el niño o niña acosado puede no saber cómo se obtuvo.

2. Con fase previa de generación de confianza En este caso, el material es entregado por el chico o chica, y la confianza se vuelve el instrumento indispensable. Para generar esa confianza el adulto se vale de distintas herramientas para mentir sobre su identidad y hacerse pasar por un par (chico o una chica menor). Esto lo logra manipulando o falsificando fotos o videos, y manteniendo conversaciones en un lenguaje coloquial acorde a la edad del chico o chica que quiera acosar. También suele tomar los gustos y preferencias que los chicos vuelcan en la web para producir una falsa sensación de familiaridad o amistad. Es frecuente que quien realiza el abuso utilice el tiempo para fortalecer e intensificar el vínculo. El tiempo transcurrido varía según los casos, pero el abusador puede lograr su objetivo en una charla o esperar meses e incluso años. Esto ayuda a que el chico se olvide o deje de tener presente que del otro lado hay un desconocido, porque a partir del tiempo transcurrido y las conversaciones compartidas pasa a considerarlo un amigo.

Una vez que el material llega al abusador, se genera una situación de chantaje donde suele quedar en evidencia la mentira sobre la identidad del adulto, quien le pide al chico más imágenes (o incluso un encuentro personal) a cambio de no mostrar el material. La posición de poder en la que se encuentra el abusador se refuerza por el manejo de la situación que tiene como adulto, y por la vergüenza que siente el chico al enterarse de que se expuso ante alguien más grande, que puede hacer público el material privado. Es necesario destacar la importancia que tiene la cámara web, ya que se vuelve indispensable, en muchos casos, para que el chico se exhiba ante el adulto. Como explicábamos anteriormente, los abusadores se valen de programas que producen un falso video para aparentar ser un o una joven.

Componentes y fases del grooming

Amistad. Contacto y acercamiento.

Contacto para conocer gustos, costumbres y rutinas de los chicos. El acosador se vale de herramientas para mentir sobre su edad al entrar en contacto con el chico: mostrar fotos o videos falsos, o bien modificados por programas web. El objetivo es mostrarse como un par con quien pueden hablar de temas íntimos.

Relación. Generación de confianza y obtención del material.

Se busca ganar confianza. Para lograr este objetivo, por medio de extensas y continuas conversaciones, se apunta a generar confesiones íntimas y privadas, que pueden tomar más o menos tiempo. El acosador suele intentar lograr empatía respecto a los gustos y preferencias de las víctimas. De esta manera el acosador consigue el envío del material con componentes sexuales o eróticos.

Componente sexual. Chantaje y acoso.

El material entregado por el chico o chica se vuelve luego objeto de 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 (plataformas de intercambio de vídeos, redes sociales, foros u otros) o enviarla a los contactos personales del niño o niña.

A continuación detallamos algunos puntos que los adultos deben trabajar con niños, niñas y adolescentes:

- Tener una actitud activa y presencial. Como familia y docentes, durante el uso de internet por parte de los chicos. Es necesario que los padres tengan presencia en su vida on- line. La charla y el conocimiento sobre las páginas web, las redes sociales, aplicaciones que usan frecuentemente, y la gente con quien interactúan los chicos es indispensable. Así como conocen sus rutinas de la escuela, el club o la calle, es fundamental saber qué gustos y rutinas tienen en su vida online.

- Acompañar a los jóvenes. Si bien los adultos sienten muchas veces que saben menos que sus hijos respecto al uso de las TIC, esto no debe evitar que los acompañen. Para los chicos es clave sentir que pueden confiar en los adultos y compartir sus experiencias.

- Confiar en sus hijos. Desde ningún punto de vista apoyamos la violación a la intimidad de los chicos (ingresar a escondidas a sus cuentas o casillas de mail). La generación de confianza es una vía de doble sentido, que hará al mismo tiempo que los chicos y chicas confíen en los adultos a la hora de necesitar acompañamiento o realizar consultas.

- Distinguir entre niños y adolescentes. Seguramente, los más chicos pueden necesitar un mayor grado de presencia. En estos casos, ante la incertidumbre de qué es lo mejor para hacer, vale la pena comparar con otras decisiones, por ejemplo: ¿a qué edad los chicos pueden volver solos del colegio? Para este tipo de preguntas no hay una única respuesta, sino que cada padre lo resolverá según la madurez del chico y la relación que tengan con él. En internet ocurre lo mismo: el padre desde su presencia debe pensar para qué está listo su hijo o su hija. En cualquier caso, creemos que la participación debe ser desde la educación y la compañía.

- Trabajar la noción de anonimato y falsa identidad en la web, explicándoles lo fácil que es abrir un perfil con datos falsos. La identidad en internet no es fácil de corroborar como lo es en el contacto cara a cara. Los chicos nacieron con un universo donde los amigos pueden ser tanto los del colegio o los del barrio, como los del chat, Facebook u otra. Saber cómo configurar la privacidad y la seguridad de las cuentas, para así poder realizar estas acciones junto a los chicos y chicas y poder elegir con quien comparten la información que publican.

- Evitar que les roben la información comprometedora. Para eso es necesario configurar y mantener la seguridad de los dispositivos.

- Tener una política cuidadosa de uso de contraseñas. Es necesario colocar contraseña en todos los dispositivos (teléfono celular, tableta, netbook, notebook o computadora de escritorio). Utilizar contraseñas seguras: lo recomendable es que combinen números y letras. Que sean fáciles de recordar, pero difíciles de robar, evitar datos predecibles como el nombre y la fecha de nacimiento, 12345, DNI o el nombre más 1234. Es importante no compartirlas (a excepción de los niños, a

quienes les recomendamos que compartan las contraseñas con sus papás, los adolescentes deben evitar compartirla, incluso con amigos). También es importante evitar usar la misma contraseña para todas las cuentas ya que si alguien accede a una, podrá ingresar a todos los espacios donde se la use.

¿Cómo detectar y qué hacer ante un caso de grooming?

Una de las principales recomendaciones para detectar si un chico o chica es víctima de grooming u otro tipo de acoso u hostigamiento es prestar atención a sus cambios de conducta o humor. Si un chico presenta repentina tristeza, angustia, descenso en el rendimiento escolar o necesidad de soledad, es necesario charlar en confianza para entender qué le ocurre ya que podría estar siendo víctima de alguna de las situaciones nombradas.

Si se detecta un posible caso de grooming, la primera medida que un adulto debería tomar es charlar con la víctima, sin avergonzarla o culparla.

Recordemos que la vergüenza del chico es el poder que el abusador tiene. Por ende, el adulto al que se recurra debe evitar afianzar esa vergüenza y permitirle al chico contar lo que le pasó con la mayor sinceridad y libertad posible. Debe evitarse la revictimización, es decir, echarle la culpa de lo ocurrido,

Como así también evitar interrogarlo en diferentes ámbitos y obligarlo a contar muchas veces lo que ocurrió.

Guardar las pruebas del acoso. Es necesario no borrar conversaciones y fotografiar o capturar la pantalla y almacenar esta información en algún dispositivo. Las fotografías enviadas por el acosador podrán proveer datos útiles para una futura investigación (marca, modelo y número de serie de la cámara, fecha y hora en la que se tomó la foto, si fue retocada, el programa usado para hacerlo y datos sobre la computadora donde se la cargó, etc.).

¿Cómo prevenirlo?

- No compartir material comprometedor.
- No hablar con desconocidos.
- Tener un perfil privado en las redes.

¿Qué hacer si te pasa?

- Hablar con un mayor de confianza.
- No borrar las conversaciones, se usarán de prueba.
- No denunciar el perfil del acosador para no perder su rastro.

Construcción de ciudadanía digital

Ciudadanía digital

Es un concepto que está en permanente construcción. Refiere principalmente a nuestras actitudes en los espacios digitales, y al mismo tiempo a nuestros derechos y obligaciones. La ciudadanía digital es un conjunto de competencias que faculta a los ciudadanos a acceder, recuperar, comprender, evaluar y utilizar, para crear, así como compartir información y contenidos de los medios en todos los formatos, utilizando diversas herramientas, de manera crítica, ética y eficaz con el fin de participar y comprometerse en actividades personales, profesionales y sociales. Debemos comenzar por comprender que el espacio online ya no es más, como en los comienzos, un lugar superficial y separado de nuestra cotidianeidad, donde los límites con lo offline eran claros y rígidos. Por el contrario, lo digital penetró en nuestras vidas filtrándose en casi todos los aspectos de nuestro día a día: trabajar, estudiar, divertirse, investigar, conocer gente, aprender oficios, jugar, pelearse, enamorarse, viajar, y tantos otros. Ya no existen horarios o dispositivos pautados de conexión, sino una penetración tal de lo digital que vuelve casi imposible dividir lo offline de lo online, convirtiendo nuestros espacios en mixtos. Luego de comprender esta nueva característica digital de lo cotidiano, debemos repensar algunas definiciones clásicas, como la de ciudadanía. Si históricamente se pensó a la ciudadanía acotada a un país o territorio, el espacio digital pone en jaque este concepto y plantea algunos interrogantes: ¿Tenemos derechos en el espacio online? ¿Son los mismos que tenemos en los offline? ¿Tenemos obligaciones de comportamiento en la web?

Una de las principales características de la web es que no tiene un recorte geográfico, es decir, no tiene límites territoriales. Entonces ¿cómo convivimos todos en este espacio? ¿Debemos construir reglas? ¿Va en contra de la filosofía de internet intentar generar normas de convivencia? Lo decidamos o no, ya existe una forma de convivir en la web, donde se ponen en juego características y elecciones de cada usuario. Se vuelve entonces indispensable conocer qué derechos y obligaciones tenemos en internet como usuarios. La UNESCO propone pensar la ciudadanía en ámbitos digitales desde tres niveles: el sujeto como receptor, como participante y como actor activo, siendo este capaz de identificar en cada nivel tanto las oportunidades como los riesgos correspondientes. Por lo tanto,

podemos sostener que para avanzar en la búsqueda de una ciudadanía digital es necesario fomentar que las personas-usuarios de tecnologías digitales sean sujetos críticos, proactivos y conscientes de las oportunidades y riesgos que existen en las TICs. Jones y Mitchell advierten al respecto que "La destreza tecnológica ya no remite al uso diestro de los dispositivos, sino que demanda un desempeño óptimo en el entorno digital en términos de participación, respeto, intercambio, colaboración y convivencia con otros". Es decir que debemos estimular conductas online responsables y participación ciudadana en prácticas cívicas en la red.

Convivencia digital

Uno de los puntos más importantes para pensar la ciudadanía digital es comprender que nuestras actitudes online hablan de nosotros. Los valores con que contamos valen tanto para espacios digitales como analógicos. Si entendemos que ser agresivo puede lastimar a otro, lo sostenemos tanto para una pelea en la calle como una en un chat. Si sabemos que podemos humillar a alguien haciendo público un secreto vale igual con un pasacalle que con un posteo. Todas estas actitudes van formando lo que entendemos por convivencia social y digital. Observamos muchas veces cierta laxitud respecto de los comportamientos digitales de adultos y niños. Internet crea un espacio donde muchas veces suelen verse comportamientos o actitudes que no se verían en la vida "real". En algunos casos sentimos que lo que se hace o dice en la web es menos grave o dañino. Para comprender este fenómeno hay que tener en cuenta algunos factores que lo alimentan: el anonimato, la ausencia física del otro y por ende, la desconexión con sus sentimientos y expresiones, la asincronicidad de las charlas o intercambios, donde se pueden confundir diálogos con monólogos intercalados, y la soledad desde la cual se escribe o postea. Todo esto hace que nuestras actitudes y acciones online se midan con una vara ética distinta que las offline. Sin embargo, es necesario recurrir a la empatía para comprender las consecuencias de nuestros actos. Ponerse en el lugar del otro es indispensable para entender cuando lastimamos y agredimos, y cómo lo hacemos. Un simple ejercicio de intercambio de roles, al menos imaginario, puede servir para dejar de publicar algo y así evitar lastimar a otros. También es necesario pensar los paralelismos con nuestras actitudes cara a cara, y analizar las interacciones online ¿diría esto si tuviese a la persona en frente?

¿Mostraría esta foto en la escuela? ¿Usaría estas palabras para responder en una discusión cara a cara? Estos simples ejercicios son clave para trasladar nuestros valores a la web y comprender que somos una misma identidad: la offline y la online. Derechos digitales Hablar de ciudadanía es hablar de derechos. Cada país establece, a partir de su constitución, qué derechos tienen sus ciudadanos. Internet, tal como mencionamos, no tiene límites ni fronteras y tampoco una constitución ni un Estado que la haga valer. Entonces ¿cómo establecemos nuestros derechos? Dijimos que la ciudadanía digital es un concepto aún en formación. Para comenzar a abordarla, debemos tomar las convenciones internacionales sobre derechos humanos y comprender que tienen vigencia en todos los ámbitos, incluida la web. En este sentido es conveniente considerar la Resolución de las Naciones Unidas que

llama la protección de los derechos humanos en internet. El Consejo de Derechos Humanos allí reconoce que los mismos derechos que las personas tienen en el mundo offline deben ser protegidos en internet. En particular se habla de: garantizar la libertad de expresión, promover la alfabetización digital, el acceso a internet como herramienta para la promoción del derecho a la educación, y también el acceso para reducir brechas digitales, la toma de medidas apropiadas para incluir a las personas con discapacidades, y atender a las preocupaciones sobre seguridad y privacidad en internet.

Legislación en argentina acerca de internet

En nuestro país existen una serie de leyes que se ocupan de legislar sobre determinados temas específicos que suceden en internet, a saber:

Ley n° 26.388 de ciberdelitos, del año 2008: conocida como "Ley de delitos informáticos", modificó el Código Penal. Agregó los delitos de distribución y tenencia de pornografía infantil por cualquier medio (art. 128); interceptar comunicaciones y sistemas informáticos (art. 153); el acceso no autorizado a un sistema informático (art. 153 bis); la publicación de correspondencia o comunicaciones electrónicas privadas (art. 155); y el acceso a bancos de datos personales (art. 157 bis), entre otros.

Ley n° 26.904: incorpora el artículo 131 al Código Penal y la figura de grooming o ciberacoso sexual que pena con prisión de 6 meses a 4 años a quien a través de las TIC contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad física de la misma.

Ley n° 25.326 de protección de datos personales, junto con el artículo 43 de la Constitución Nacional (habeas data), protege la información personal de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, y explicita la confidencialidad del responsable del tratamiento de los mismos (incluyendo la protección de la privacidad e intimidad en internet).

La huella digital

La información en las redes es difícil de borrar y controlar, por eso es importante cuidar todo lo que se publica o comparte. Cuando utilizamos internet construimos una huella digital, es decir, el rastro que dejan nuestras actividades como fotos, videos, publicaciones y comentarios. Así, toda la información que está en la web y que se asocia con nuestro nombre se convierte en la manera que tienen terceros para conocernos más y forman parte de nuestra identidad digital. La huella digital incluye las publicaciones que un usuario realiza, aquellas en las que sea etiquetado o mencionado, las fotos o videos personales o subidos por otros, las páginas web donde se cite su nombre, las cuentas de usuario en redes sociales

que estén asociadas a su nombre real, las noticias referidas a su persona, y la participación como usuario en foros, salas de juegos, de chat u otros.

Es importante considerar que, una vez que un dato o una imagen son subidos a la web, es difícil de borrar ya que en internet no hay olvido. Además, pese a que el usuario puede borrar una publicación, no se elimina la totalidad de esa referencia, dado que otra persona pudo haber descargado, compartido o guardado el posteo o el contenido y, por lo tanto volver a subirlo y compartirlo. Es decir, perdemos el control de nuestro dato personal. Por eso, siempre se recomienda pensar dos veces antes de compartir información personal, ya que quedará publicada en la web y será difícil de borrar si el día de mañana queremos hacerlo.

Riesgos para la identidad digital

El principal riesgo cuando no se cuida la huella digital es brindar información privada, actual o del pasado, a personas que no tendrían por qué recibirla. Cuando se brinda información privada o íntima en un ámbito público como es internet sin ajustar la configuración de las cuentas, la persona se expone a ser asociada con información que tiene sentido en un ámbito privado pero otro diferente en el público. Se corre el riesgo de que 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 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.

Relevancia de la identidad digital

En la actualidad, internet es la fuente principal de información para conocer a alguien. Ya sea por medio de un sitio o página web, o bien por redes sociales, brinda la posibilidad de acceder a información personal de quien se busque. Por eso es primordial el cuidado de lo que se sube, ya que internet será la vidriera mediante la cual el mundo nos conocerá. Por ejemplo, en el caso de la búsqueda laboral, si bien cuando se busca empleo se debe presentar un currículum vitae armado por uno mismo, la penetración de internet permite que el empleador se pueda valerse de la información que existe en la web y buscar referencias allí del perfil a analizar. Para hacerlo, escribe el nombre en cuestión en los buscadores y analiza todas las referencias que aparezcan. Si el usuario nunca configuró la privacidad y seguridad de sus cuentas en las redes sociales, toda la información que haya subido allí

estará al alcance de quien la busque, ya que la primera respuesta del buscador será el perfil del usuario en Facebook, Twitter, Instagram u otra red social desde donde podrán indagar en las publicaciones que ese usuario ha hecho desde que abrió la cuenta. Muchas veces lo que se sube online son cuestiones privadas e íntimas que refieren a un contexto específico y, tal vez, al ser vistas por un posible jefe, pueden perder sentido y ser entendidas como algo negativo a la hora de evaluar la aplicación a un trabajo.

Ciberbullying

Es el hostigamiento online por parte de pares. Al hablar de hostigamiento hacemos referencia a aquellas situaciones en las que uno o varios niños son marginados, discriminados, maltratados por parte de uno o varios pares de manera sostenida en el tiempo. Una práctica que no es propia o generada por lo digital, pero que encuentra en estos ámbitos un lugar de reproducción.

El hostigamiento virtual consiste en el acoso entre pares e incluye las conductas hostiles sostenidas de forma reiterada y deliberada por parte de un individuo o grupo con la finalidad de producir daño a otro, mediante la utilización de tecnologías de la información y comunicación. El ciberbullying puede definirse como “el uso de medios telemáticos (internet, celulares, videojuegos online, aplicaciones, etc.) para ejercer el acoso psicológico entre iguales”. Es decir, tiene que haber niños, niñas y adolescentes en ambos extremos del conflicto para que sea considerado como tal. Si hay presencia de un adulto, estamos ante otro tipo de ciberacoso. En otras palabras, es todo acto discriminatorio que se da entre chicos y chicas en el ámbito de las TICs. Comprende entonces casos de ciberacoso en un contexto en el que únicamente están implicados niños, niñas y adolescentes y supone la difusión de información, de datos difamatorios y discriminatorios a través de dispositivos digitales como aplicaciones, mails, mensajería instantánea (Whatsapp). Además, los registros de navegación guardan datos (memoria caché), por lo que no hay certeza de la desaparición de la información. Esto hace que el daño causado sobre quien sufre el acoso no tenga un final establecido y continúe reproduciéndose. La discriminación existe tanto en los espacios online como en los offline. Por ende, es discriminatoria toda distinción, restricción, o preferencia basada en motivos de una supuesta raza, religión, nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos que tenga por objeto anular o menoscabar el reconocimiento y ejercicio en condiciones de igualdad de los derechos humanos y libertades fundamentales en las esferas políticas, económicas, sociales, culturales o en cualquier otra esfera de la vida pública. El hostigamiento online tiene la particularidad de permitir el sostenimiento del acoso u hostigamiento a toda hora y desde cualquier sitio, es decir son conductas sistemáticas no aisladas. Provocando que, por lo general, el efecto en la persona que está siendo discriminada sea mayor. A su vez, al tratarse de una acción en espacios públicos como las redes sociales, tienen mayor alcance (más usuarios lo ven).

Como se mencionó, cuando se sube información a la web, se puede perder el control sobre quién lo comparte o guarda y por ende, de cuántas personas conocen lo que publicamos. Si uno discrimina mediante un posteo o bien crea un grupo o un hashtag, dependiendo de la red social, esto podría causar mayor perjuicio para el acosado ya que la información difamatoria se podría viralizar fuera del círculo conocido, potenciando el daño a la imagen. Además del alcance exponencial que permiten, internet y las redes sociales presentan el riesgo de la falta de empatía, por lo que pueden invitar o animar a participar del acoso a personas que no lo harían en forma personal. La falsa sensación de anonimato suele ir acompañada por una minimización del problema y su importancia. Esto puede causar que un mayor número de usuarios se sume al acoso, agrandando el círculo de discriminadores. La falta de empatía al no registrar el efecto de la discriminación en el otro, puede permitir el acceso de un mayor número de usuarios a este tipo de conductas. Otra característica del hostigamiento digital son las múltiples pantallas por las que sucede. Las TICs ofrecen una amplia variedad de canales para realizar el acoso, como pueden ser mensajes personales, grupos en redes sociales, memes (fotos con texto incitando a la burla), imágenes o videos difamatorios. Esto reproduce el daño ya que se combinan los dispositivos y se multiplican los canales de difusión y recepción. Entonces, el anonimato, la no percepción o registro del daño causado a otro, y la posibilidad de viralización hacen que el ciberbullying sea un tema a tratar tanto en el ámbito familiar como en las escuelas.

El alcance del ciberbullying

El cyberbullying tiene algunas semejanzas con el bullying tradicional (discriminación), pero también tiene características propias que es fundamental conocer para poder trabajar en la búsqueda de una convivencia social-digital pacífica y libre de discriminación. Fundamentalmente deben tener en cuenta que se trata del espacio público. Los chicos y las chicas en muchos casos no tienen noción sobre el alcance que puede lograr una publicación que se realiza en internet o redes sociales. Estos ámbitos digitales producen una expansión de contenidos provocando que desconocidos u otros accedan a la publicación realizada. Como ya se dijo, en internet no existe el derecho al olvido. Una vez que la información está online es muy difícil de borrar, ya que por más que se elimine lo publicado si otro usuario lo guardó, la información seguirá reproduciéndose.

Discurso del odio y respeto digital

Cuando hablamos de trasladar valores morales y éticos a internet, nos referimos a proyectar nuestra forma de ser y educación a los espacios online, donde nos expresamos, opinamos, charlamos y producimos. Es decir, si no fomentamos el odio ni la agresión en espacios cara a cara, debemos evitar hacerlo en internet. Sin embargo ¿qué pasa cuando en los espacios online proyectamos el odio, agresión o violencia que realmente tenemos?

¿Cómo se trabaja cuando la web se vuelve reflejo del odio de la sociedad? En internet existe agresión, discriminación y también el fenómeno del discurso del odio. Este tipo de discurso refiere a una forma de expresión deliberada que tiene como objetivo denigrar, humillar o discriminar a un grupo de individuos, sea por su raza, nacionalidad, orientación sexual, u otro tipo de característica específica. Está asociado a la xenofobia, al racismo y al nacionalismo extremo. Como la mayoría de los problemas sociales históricos, el discurso del odio se expresa también a través de internet.

Es lógico pensar que así suceda, ya que la web se convirtió en la principal vía de expresión y comunicación actual. Para analizar este fenómeno y la violencia digital en general, es necesario plantear algunos puntos:

- El discurso de odio, como toda forma de agresión, precede a la web. Por ende, hay que focalizar en la raíz del problema y no en su vía de comunicación. Es indispensable educar en el respeto hacia el otro y en el buen uso de la web, evitando caer en una mirada negativa sobre internet. Es necesario ir a la raíz del problema, que es el odio hacia lo distinto o diverso, para –desde la educación– prevenir y reparar.

- Internet no lo crea pero lo fomenta. Si bien estos fenómenos de agresión dijimos que preceden a la web, es cierto que algunas características de los espacios digitales fomentan la agresión como el anonimato, la soledad, la falta de presencia física del otro y la facilidad para opinar y compartir, que vuelve más accesible cierto discurso agresivo o violento. Es importante entonces educar y trabajar sobre lo grave que es el hostigamiento online y la responsabilidad que acarrea hacerlo: los daños y perjuicios que puedo provocar a otros/as.

Formas, roles y consecuencias del ciberbullying

El ciberbullying puede darse de diferentes formas e involucra diversos roles (con perfiles asociados), que esquematizamos a continuación.

Acoso

Envío de imágenes denigrantes, seguimiento a través de software espía, envío de virus informáticos, elección en los juegos online de un jugador con menos experiencia para ganarle constantemente y humillarlo, entre otros.

Manipulación

Uso de información encontrada en las plataformas para difundirla de forma no adecuada entre los miembros, acceso con la clave de otra persona a un servicio y realización de acciones que puedan perjudicarlo en su nombre, entre otros.

Exclusión

Denegación a la víctima del acceso a foros, chat o plataformas sociales de todo el grupo, entre otros

Los roles tradicionales de la discriminación varían cuando sucede en las redes sociales o internet. La falsa sensación de anonimato, de la mano de la soledad en la que suele establecerse la conexión, permite que quienes no se animan a discriminar en forma personal, tengan más facilidades para hacerlo vía web, ya sea compartiendo imágenes, con un “me gusta” a cierta publicación o comentando publicaciones discriminatorias que entran en el escenario del hostigamiento online.

Es importante analizar los perfiles y roles descriptos teniendo en cuenta su dinamismo. En ese sentido, recomendamos evitar la asociación de un niño, niña o adolescente con un perfil para no caer así en estigmatizaciones que vuelven estáticas identidades que son momentáneas. En la práctica los chicos y chicas recorren varios de los perfiles y pasan de acosador a acosado en poco tiempo. Por lo tanto, aconsejamos conocer las características de los diversos roles recordando que son descripciones de situaciones y no de identidades. En el mismo sentido cabe recordar que los protagonistas de las situaciones descriptas son niños o niñas y, por consiguiente, sujetos de derecho y participación. Es necesario entonces acompañar, dialogar y cuidar tanto al niño o niña que está siendo acosado como al que está acosando. Cualquier tipo de discriminación acarrea como principal consecuencia la humillación para quien es agredido. Sin embargo, al producirse en un espacio público como internet, las consecuencias se potencian y expanden. Es importante saber los efectos y el alcance que genera para prevenir y educar a partir de sus particularidades.

- Cuando se produce la humillación en forma personal, responde a un contexto tanto de la vida del acosador como de la de los ayudantes y de la víctima. En internet y debido al no olvido de las publicaciones, este recorte temporal se pierde y la información perdura más allá de los contextos de los protagonistas. Esta característica hace que las consecuencias se extiendan y generen una constante relación entre ese hecho y los participantes, más allá de que se hayan arrepentido (en el caso del acosador o ayudantes) o que hayan podido superar lo ocurrido (en el caso

de la víctima). Este es un punto central donde el adulto debe actuar. Ya sea si el cercano es un niño agresor o si es un agredido, es necesario recordar que al producirse en internet, el acoso se vuelve un sello que perdurará en su reputación online en el presente y en el futuro. Es fundamental trabajar el tema a partir de ejemplos concretos, como puede ser una futura búsqueda laboral donde la agresión se vuelva un antecedente que un posible jefe vaya a tener en cuenta. Estos ejemplos pueden ser útiles para evitar la participación en las discriminaciones web.

- La expansión y viralización del contenido logra que el dato o información difamatoria llegue a más personas que las estipuladas y por ende se extienda el efecto de la humillación. La falta de olvido en la web hace que el acto discriminatorio se sostenga en el tiempo.

- Registro de su accionar y asociación de lo hecho con su perfil tanto en el presente como en el futuro. Es decir, todo lo que un perfil de usuario pública quedará asociado en su reputación web o identidad digital, como se explicó en el apartado anterior.

Sexting

Viralización de imágenes y contenidos inadecuados: muchas veces jóvenes (y adultos) producen contenidos de índole sexual, como fotos o videos íntimos, que no están destinados a la circulación pública. Sin embargo, diversas circunstancias pueden derivar en su difusión en redes sociales o web. Aportamos algunas recomendaciones, cuidados y recursos para la denuncia y asesoramiento.

La palabra sexting viene de la combinación en inglés de las palabras sex (sexo) y texting (texteo, envío de mensajes de texto mediante teléfonos móviles). La práctica surge del uso de tecnologías digitales y consiste en la circulación de un contenido sexual a través de dispositivos móviles (celulares, tabletas) y que se da mediante diversas aplicaciones (Whatsapp, Facebook, Instagram, Twitter, Snapchat, etc.). Es decir, el envío de imágenes y vídeos sexuales no solo vía mensaje de texto sino, también, mediante mensajería instantánea, foros, posteos en redes sociales o por correo electrónico. De este modo, la imagen es enviada a uno o varios contactos que, a su vez, pueden reenviarla y comenzar la viralización. Este tipo de información estará estrechamente ligada con la identidad digital de la persona que retrate, siendo por eso importante conocer las herramientas necesarias para usar la tecnología de manera responsable y, si se quiere realizar esta práctica, hacerlo de manera segura.

Sexting, viralización de imágenes y contenidos íntimos

Una de las prácticas entre los jóvenes con el uso de tecnología es la producción de contenidos de índole sexual, principalmente fotos y/o videos íntimos.

La permanente conexión y el uso masivo de dispositivos móviles, principalmente teléfonos celulares, genera que, desde una corta edad, los chicos y las chicas tengan acceso a la recepción y al envío de imágenes y videos. A esto se suma que la adolescencia tiene una relación directa con el despertar y la curiosidad sexual. Por eso, la posibilidad de expresar deseos y fantasías sexuales mediante la tecnología es parte de la lógica histórica de los jóvenes.

La instantaneidad en las comunicaciones, propia de la época marcada por internet, permite que las fotos o videos tomados sean enviados en el mismo momento y por el dispositivo más cercano y fácil de usar. La sensación de confianza y el poco temor hacia posibles riesgos, propios de la adolescencia, acentúan las prácticas de sexting, ya que los jóvenes suelen dejar fuera de su análisis los efectos a mediano plazo del envío de imágenes privadas. Asimismo, desde los medios de comunicación, y las cuentas de personas de la farándula en las diversas redes sociales, que hacen pública su vida privada, parece darse el incentivo a realizar esta práctica.

Estamos en presencia de una de las acciones típicas del avance tecnológico: el tomarse retratos (fotos o videos) y enviarlos a otros contactos. Esta práctica ya tradicional en usuarios de las TIC se realiza principalmente a través de aplicaciones de mensajería como Whatsapp, también en redes sociales (Instagram, Facebook, Snapchat), y en sitios web, blogs, foros o sitios de compra y venta. Las cámaras están incluidas en la mayoría de los teléfonos celulares, tabletas y notebooks generando un acceso diario e instantáneo a la posibilidad de fotografiar o filmar lo que sucede alrededor nuestro.

Otra de las características de este avance es la apertura a la participación de los usuarios. La comunicación dejó de ser un monólogo donde únicamente habla el gran productor o distribuidor, para ser un diálogo casi infinito, donde muchos tienen la posibilidad de hablar, producir y expresarse. Y no solo eso, sino que también existe la respuesta ante una acción comunicacional. Es decir, un usuario publica una foto o un video e inmediatamente está la posibilidad de ver la reacción en la comunidad que responderá a ese posteo o publicación con comentarios o signos de aprobación o rechazo. Esta combinación de imágenes y participación provoca distintos efectos.

La producción de videos, la edición de fotos y la creatividad se encuentran al alcance de todos, a través de aplicaciones y programas muy variados. Antes de la expansión de internet, la producción de imágenes y de sonido era una actividad reservada a los grupos profesionales con conocimientos y equipos específicos. En la actualidad, muchos usuarios de internet tienen el rol de consumidores y productores en simultáneo. El cruce entre la circulación de las imágenes y la mayor participación de los usuarios de internet puede conducir a algunos riesgos, problemas o situaciones a tener en cuenta.

El sexting es una de las prácticas que debe considerarse a la hora de analizar el fenómeno de la circulación de imágenes en la web. Las imágenes que componen el fenómeno de sexting son obtenidas, en muchos casos, de manera voluntaria. Es decir, el

chico o la chica que aparece revelando su identidad es consciente de ello. O bien es el/ la que se filma o fotografía, o bien da su consentimiento para que otro lo haga. Esto no significa que exista un consentimiento para la divulgación de los contenidos. Existe una diferencia entre el aceptar ser tomado por una cámara y el que estas imágenes sean publicadas en espacios públicos como internet o las redes sociales. Este es uno de los grandes conflictos que existen respecto de este tema, por lo que es necesaria la intervención del adulto para dialogar junto con los jóvenes sobre la problemática.

Una característica fundamental de este tipo de contenidos es que corresponde a información (ya sea foto o video) de carácter explícitamente sexual. Otra particularidad es que, a pesar de que existe sexting en todas las edades de usuarios, es una práctica difundida entre los adolescentes.

Entonces, si bien toda la población usuaria de las nuevas tecnologías puede verse implicada en problemas por la circulación de imágenes, es importante acompañar a los niños, niñas y adolescentes en este proceso de socialización que incorpora nuevas herramientas, medios y efectos. Por eso, resulta indispensable brindar información para que los jóvenes conozcan los posibles riesgos a los que se enfrentan e incorporen estrategias de prevención y gestión en caso de ser víctimas o tener inconvenientes en este sentido. Al mismo tiempo, entendemos como irremplazable la compañía y el cuidado adulto en el mundo digital de los chicos y chicas.

Posibles situaciones de sexting

Los escenarios donde fotos o videos con contenido sexual son enviados a través de dispositivos móviles son diversos y cambian según la edad de los protagonistas, el lugar donde viven y el contexto social en el cual están inmersos. Sin embargo, podemos pensar a grandes rasgos situaciones para comprender de qué hablamos cuando hablamos de sexting.

Además, en todos los casos, existe el riesgo del robo de fotos o videos sexuales guardados en dispositivos móviles para luego publicarlos en internet. El acceso a un dispositivo por medio de un robo, de un descuido o de un hackeo es la puerta de entrada a que personas indeseadas accedan a la información guardada. En estos casos los protagonistas están de acuerdo en fotografiarse o filmarse, pero no en que este material sea enviado a terceros o sea publicado. El material privado es publicado y circula sin el control de los protagonistas, quienes ven su imagen íntima reproducirse en redes sociales y sitios web, dañando su reputación.

La porno venganza, pornografía vengativa o revenge porn, aparece como una nueva modalidad de extorsión, escrache o venganza multimedial. Por esto entendemos al contenido sexual explícito que se publica en la web o se distribuye por servicios de mensajería instantánea, sin el consentimiento del individuo que aparece en las imágenes. Existe entonces una filmación o un registro fotográfico de un acto sexual entre dos personas

adultas, de manera consensuada y voluntaria, y luego una de ellas la pública a través de una página web, o la comparte a través de una App (como Whatsapp), vía mail o red social. Los motivos por los cuales se producen estas intromisiones y/o violaciones a la privacidad e intimidad pueden ser varios, pero surge como predominante la exposición de estos registros por parte de ex parejas. Una vez que los videos o las fotos comienzan a circular, millones de usuarios desconocidos con acceso no autorizado a ese material, continúan compartiéndolo, logrando así una viralización imparable del contenido. Cabe destacar que este tipo de problemática afecta principalmente a mujeres.

Tanto los casos reportados como los que han trascendido públicamente, muestran que detrás de esta modalidad existe una cuestión de género, donde se exhibe al cuerpo de la mujer como un producto, expuesto públicamente contra su voluntad. Las consecuencias para las víctimas van desde la pérdida del derecho y el honor, hasta trastornos en su vida laboral o familiar. Cabe destacar que la viralización llega a tales grados que muchas veces las mismas familias de las víctimas acceden a esos contenidos privados o íntimos.

Otra nueva modalidad de sexting es el doxing, que toma su nombre de la contracción de la palabra en inglés documents, que significa documentos, y refiere a la práctica de investigar, recopilar y publicar información privada y personal de un sujeto, generalmente para constatar la identidad del mismo. Existen diversas variantes del doxing dependiendo de los objetivos para los cuales se realice. En este caso utilizaremos la denominación para hablar de la práctica habitual que suele verse en grupos de mensajería instantánea en donde se difunden fotos y videos de una persona (mayoritariamente mujeres) en una situación sexual privada e íntima, acompañadas de capturas de pantalla de las redes sociales, junto con otras fotos que revelan y constatan la identidad de la misma.

Es decir, que una de las principales fuentes de información para esta modalidad son las redes sociales y la información pública que los usuarios dejan en la web. Por este motivo, resulta imprescindible tomar medidas de precaución y cuidar la privacidad en cuanto a la información que se deja abierta al público en general. Tomando las medidas necesarias, y evitando compartir datos personales y publicaciones, podremos prevenir y no ser víctimas de esta problemática.

Consecuencias del sexting

Como se dijo, las imágenes que se envían en situaciones de sexting son obtenidas muchas veces en forma voluntaria y enviadas a través de diversos dispositivos. Responden a un contexto específico, íntimo y sexual. Sin embargo, cuando esa imagen sale del contexto de origen y se publica en internet, surgen consecuencias impensadas para los protagonistas.

- Descontextualización de la situación: la imagen o video tiene lógica y sentido en el contexto desde el cual se pensó. Por consiguiente, cuando se modifica esa situación y la imagen/video pasa a ser pública, los protagonistas suelen sentirse incómodos por la exposición.

- Exposición: la circulación de una imagen en la web genera que la reciban personas que no son los destinatarios originales. Cuantos más contactos vean la imagen, más expuesto/a estará el/la protagonista.

- Daño a la identidad o huella digital: un video o una foto privada expuestos en público pueden dañar la reputación web del/los protagonista/s. Como se explicó anteriormente, el hecho de que en internet sea muy difícil borrar la información permite que el material perdure a través del tiempo, exponiendo una situación que será relacionada con la identidad del protagonista en cualquier búsqueda online, presente o futura. Por esta razón, las publicaciones originadas en situaciones de sexting pueden dañar, en el presente o en el futuro, a los protagonistas del material.

Resolución 234/2016

Protocolo de actuación

Resolución 234/2016

Bs. As., 07/06/2016

VISTO el Expediente CUDAP: EXP-SEG: N° 0003372/2016, las Leyes N° 26.388 del 25 de junio de 2008, y N° 26.904 del 11 de diciembre de 2013 y,

CONSIDERANDO:

Que en el marco de la lucha contra el narcotráfico y el crimen organizado que ha asumido este gobierno resulta menester realizar todos los esfuerzos y contar con los elementos necesarios para lograr una mayor eficiencia y eficacia.

Que a nivel mundial ha tomado gran relevancia el fenómeno de la cibercriminalidad teniendo ésta una gran relación con el crimen organizado, en especial el narcotráfico, la pornografía infantil, los delitos sexuales y la venta ilegal de armas entre otros.

Que el incremento de los delitos cometidos a través de las nuevas Tecnologías de la Información y Comunicaciones (TICs) en la última década deviene en una necesidad de capacitar y dotar a las Fuerzas de Seguridad y Policiales con herramientas, métodos y procedimientos a fin de mejorar su investigación y conservar la prueba digital.

Que los delitos informáticos o ciberdelitos son actividades delictivas en donde las TICs se utilizan como medio para la comisión (estafas, extorsiones, corrupción de menores, etc.), o bien, son objetos del delito (acceso ilegítimo a sistemas o datos restringidos, daño informático, denegación de servicios, etc.).

Que los llamados ciberdelitos se encuentran contemplados en la Ley N° 26.388 sancionada en junio del año 2008 y el delito de grooming fue incorporado al Código Penal de la Nación por la ley N° 26.904 en el año 2013.

Que el anonimato que provee la utilización de Internet y las redes sociales dificulta la persecución de los delitos cibernéticos.

Que la prueba digital se diferencia de la prueba tradicional por su volatilidad, la capacidad de duplicación de la misma, la facilidad para alterarla y la cantidad de metadatos que posee.

Que la investigación de la delincuencia informática se dificulta debido a la intangibilidad y volatilidad de la evidencia digital, por lo que su adecuada preservación es fundamental para que las mismas sean admitidas judicialmente.

Que la prueba digital, en su estado natural, no permite entrever qué información es la que contiene en su interior, por lo que resulta para ello ineludible, examinarla a través de instrumentos y procesos forenses específicos.

Que la prueba digital es fundamental para la investigación por la información y datos de valor que pueden extraerse de los distintos dispositivos electrónicos, tanto aquellos aportados por el denunciante como los que se encuentren en el lugar de allanamiento.

Que dicha prueba puede ser en ciertos delitos de extrema preponderancia y en algunos casos, la única evidencia que se puede obtener para el esclarecimiento del delito investigado.

Que la adecuada obtención, conservación y tratamiento de la evidencia digital es un elemento clave para asegurar el éxito de las investigaciones.

Que las Fuerzas de Seguridad y Policiales deben estar capacitadas para operar con prueba digital teniendo en cuenta su fragilidad ya que las altas temperaturas, la humedad y cualquier error en su manejo puede acarrear la destrucción de la misma.

Que incluso el valor de las pruebas obtenidas con el mayor esmero puede perderse si no se respeta debidamente la cadena de custodia, las precauciones especiales al momento de recolectar, manipular, documentar y examinar la evidencia digital ya que de no hacerlo, podrían generarse nulidades judiciales o resultar imprecisa a efectos de esclarecer el hecho delictivo.

Que es necesario asistir y capacitar a las Fuerzas de Seguridad y Policiales dado que son las encargadas de auxiliar en la investigación de estos delitos, y que dicha investigación requiere de una experiencia, herramientas y actuación distinta que en los delitos convencionales.

Que es fundamental que las Fuerzas de Seguridad y Policiales sean capaces de reconocer qué tipo de dispositivos pueden contener información vital para la investigación del delito para su posterior secuestro.

Que resulta necesario que se trabaje mancomunadamente con Organizaciones No Gubernamentales que tienen finalidad de prevención y erradicación de delitos como el Grooming, siendo estas una fuente de datos importantes, por su rol protagónico frente delitos de esta índole.

Que el presente protocolo tiene por objeto concientizar sobre las prácticas a seguir en la investigación del delito estableciendo los principios a tener en cuenta al momento de la investigación, además de abarcar la índole, pertinencia, modo de obtención, conservación y tratamiento de las evidencias digitales, desde la actuación de los agentes de prevención hasta la entrega de las mismas para su análisis.

Que además, pretende que los agentes de las Fuerzas Policiales y de Seguridad, comprendan la importancia de su labor y las consecuencias que se generan al no aplicar los principios que aquí establecidos.

Que la SUBSECRETARÍA DE ASUNTOS JURÍDICOS ha tomado la intervención de su competencia.

Por ello,

LA MINISTRA DE SEGURIDAD RESUELVE:

Artículo 1°. *Apruébese el "PROTOCOLO GENERAL DE ACTUACIÓN PARA LAS FUERZAS POLICIALES Y DE SEGURIDAD EN LA INVESTIGACIÓN Y PROCESO DE RECOLECCIÓN DE PRUEBAS EN CIBERDELITOS" que, como ANEXO forma parte integrante de la presente resolución.*

Artículo 2°. *Invítese a las Provincias y a la CIUDAD AUTÓNOMA DE BUENOS AIRES a adherir al presente Protocolo.*

Artículo 3°. *Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.-*

Dra. PATRICIA BULLRICH, Ministra de Seguridad de la Nación.

Anexo

PROTOCOLO GENERAL DE ACTUACIÓN PARA LAS FUERZAS POLICIALES Y DE SEGURIDAD EN LA INVESTIGACIÓN Y PROCESO DE RECOLECCIÓN DE PRUEBAS EN CIBERDELITOS.

I. Reglas generales, definiciones y principios

***1. Objeto**: El presente PROTOCOLO GENERAL DE ACTUACIÓN (en adelante "PGA") tiene por objeto establecer las pautas y el procedimiento al que deberán atenerse los miembros de las Fuerzas Policiales y de Seguridad al momento de la investigación y proceso de recolección de pruebas en el marco de los ciberdelitos y en especial en el delito de grooming contemplado en el artículo 131 del Código Penal de la Nación.*

***2. Generalidades:** El presente PGA es de aplicación obligatoria en todo el país para todo el personal de GENDARMERÍA NACIONAL ARGENTINA, PREFECTURA NAVAL ARGENTINA, POLICÍA FEDERAL ARGENTINA Y POLICÍA DE SEGURIDAD AEROPORTUARIA, debiéndose tener en cuenta que su accionar debe ajustarse en un todo a la Constitución Nacional, las leyes penales, las pautas procesales y los protocolos vigentes.*

***3. Definiciones**: A los fines del presente PGA se entiende por:*

***3.1. Ciberdelito**: todo delito en donde las Tecnologías de la Información y las Comunicaciones (TICs) sean utilizadas como medio para la comisión del mismo o bien sean el objeto.*

***3.2. Grooming**: delito que se configura cuando por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, se contacta a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*

***3.3. Copia Forense**: réplica en forma completa (por sector, bit a bit) de la estructura y contenido de un dispositivo de almacenamiento. Se conecta un dispositivo externo al dispositivo y se hace la copia idéntica. Puede realizarse por medio de un copiador de hardware o un software.*

***3.4. Hash**: es una función matemática que permite representar datos de longitud variable como un dato de longitud fija y donde pequeñas diferencias en los datos de entrada generan una gran diferencia en los datos de salida. Los valores resultados también se denominan hash (singular) o hashes y permiten identificar con gran nivel de precisión los datos originales, sin revelar el contenido real de los mismos a través de una función unidireccional. Tiene como funciones primordiales la identificación y el control de la integridad de los datos, resultando de vital importancia a los fines de controlar la preservación de la cadena de custodia y evitar planteos de nulidad.*

***3.5. Evidencia digital**: es la prueba fundamental en los ciberdelitos. Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Dicha prueba se adquiere cuando se secuestra y asegura para su posterior examen. Normalmente las pruebas consisten en archivos digitales de texto, vídeo o imagen, que se localizan en ordenadores y todo tipo de dispositivos electrónicos*

3.6. Allanamiento*: es el acto procesal que implica el ingreso a un domicilio, recinto de acceso restringido u otro lugar dentro del marco de una investigación criminal, consistente en el registro del mismo. Este acto se realiza mediante el uso de la fuerza pública en horario hábil y con las excepciones horarias que autoriza la ley, procurando minimizar los riesgos a la integridad física de la totalidad de los actores y procurando la preservación de los medios de prueba buscados.*

3.7. Requisa Personal: *es una medida procesal de coerción real por medio de la cual se procura examinar el cuerpo de una persona y las cosas que lleva en sí, consigo, dentro de su ámbito personal o en vehículos, aeronaves o buques, con la finalidad de proceder a su secuestro o inspección por estar relacionadas con un delito*

3.8. Secuestro*: es una medida procesal por el cual se procede a la retención de lo que se hallare en virtud de un allanamiento o de una requisa personal dejando constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o fiscal intervinientes.*

Los elementos de prueba serán recolectados según las reglas aplicables al tipo de objeto, garantizando la cadena de custodia.

3.9. Cadena de Custodia: *es el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso.*

3.10. Dirección IP*: La dirección IP, acrónimo para Internet Protocolo, es un número único e irrepetible con el cual se puede identificar el acceso a internet de cualquier dispositivo con conectividad.*

II. Principios generales de intervención

1. Accesibilidad y respeto*: Los agentes de las Fuerzas Policiales y de Seguridad están obligados a tratar a la víctima con absoluto respeto por sus derechos y garantías constitucionales, otorgándole especial atención y seguridad al tratarse de víctimas en situación de vulnerabilidad y sensibilidad.*

2. Interés superior del niño*: Cuando se trate de víctimas menores de 18 años, el vector de actuación de las Fuerzas Policiales y de Seguridad debe velar siempre por el interés superior del niño. Por interés superior del niño se entenderá al conjunto de acciones y procesos tendientes a garantizar un desarrollo integral y una vida digna, así como las condiciones materiales y afectivas que les permitan vivir plenamente y alcanzar el máximo de bienestar posible.*

3. Confidencialidad y privacidad: *En todo momento, debe respetarse la privacidad de la víctima, no pudiendo dar publicidad de sus circunstancias personales, declaraciones y/o fotografías.*

III. Principios específicos de intervención

1. Recolección, Aseguramiento y Transporte: *Los procesos de recolección, aseguramiento y transporte de la prueba no pueden en ningún caso modificar la original.*

2. Examen por Expertos: *La evidencia digital sólo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito.*

3. Documentación de las Actuaciones: *Todo lo actuado durante el proceso de recolección, transporte y almacenamiento de la prueba tiene que estar completamente documentado, preservado y disponible para un posterior examen.*

4. Prevención: *A los fines de la investigación de los ciberdelitos alcanzados por el presente protocolo las Fuerzas Policiales y de Seguridad podrán hacer y solicitar el uso de las técnicas de investigación establecidas en los Códigos de Fondo, Procedimentales y leyes especiales de la jurisdicción correspondiente.*

IV. Pautas específicas de actuación

1. Denuncia

1.1 Recepción: *Las denuncias en materia de ciberdelitos, deben cumplir con lo establecido en el Código Procesal Penal de la Nación, los Códigos Procesales de cada provincia y de la CIUDAD AUTÓNOMA DE BUENOS AIRES, en cuanto a su recepción, forma, contenido.*

La denuncia puede ser receptada por cualquiera de los canales de recepción de denuncias existentes siguiendo el procedimiento normal para el trámite de la misma.

Respecto de la comunicación y procedimiento de la denuncia, las Fuerzas Policiales y de Seguridad deberán incluir obligatoriamente:

a. Lugar y fecha en que fueron iniciadas.

b. Los datos personales de quienes en ellas intervinieron.

c. Las declaraciones recibidas, los informes que se hubieran producido y el resultado de todas las diligencias practicadas.

Recibida la denuncia por cualquiera de los canales existentes, los miembros de las Fuerzas Policiales y de Seguridad deberán comunicar de inmediato al Ministerio Público Fiscal quienes a su vez, pondrán en conocimiento la denuncia en caso de tratarse del delito de grooming o pornografía infantil a la "Red 24/7".

Al momento de la recepción de la denuncia los miembros de las Fuerzas Policiales y de Seguridad deben procurar el aseguramiento de la prueba aportada por el denunciante o solicitar la misma, la cual podrá verse contenida en correos electrónicos, dispositivos electrónicos tales como computadoras, dispositivos móviles, chats de mensajería instantánea, redes sociales, páginas de internet, etc.

La conservación de la prueba por parte del denunciante consiste en el almacenamiento de las conversaciones, mensajes, imágenes, videos y cualquier otra prueba que se relacione con el hecho. Es necesaria su custodia y cuidado conforme las reglas establecidas en el presente Protocolo, a fin de que queden a disposición de la Justicia.

Si la misma consiste en correos electrónicos, se deben guardar los mismos o ser reenviados a una casilla oficial como archivo adjunto. La impresión en papel de los mismos impide rastrear el remitente original del material probatorio.

Si la prueba se encuentra almacenada en un dispositivo de telefonía celular, quien reciba la denuncia deberá tomar los recaudos necesarios para que un informático forense realice una copia forense del dispositivo móvil para su análisis y posterior estudio.

Es imprescindible que si el material probatorio se encuentra en páginas de internet, redes sociales, etc. se solicite inmediatamente a los responsables la preservación de la evidencia digital allí contenida hasta tanto se obtenga la orden judicial pertinente.

1.2. Denuncia realizada por víctima menor de edad: *En el caso que las víctimas de un ciberdelito sean menores de edad, deberán ser interrogadas por un psicólogo especialista en niños, niñas y adolescentes.*

El interrogatorio se realizará en un ambiente acondicionado a la edad y la etapa evolutiva del menor, contando con el equipamiento e implementos que sean necesarios.

En el tratamiento de las víctimas, debe evitarse cualquier conducta o actitud que tienda a la re-victimización de las mismas.

La re-victimización tiene lugar cuando a los daños que sufre una persona como consecuencia del delito del que fue víctima se suman aquellos generados por el proceso legal. Para evitar esto, no se debe juzgar y/o inferir algún grado de responsabilidad por parte de la

misma. Es decir, a los daños causados a la víctima por los delitos de los que fue objeto, no se le debe sumar el maltrato institucional.

2. Allanamiento

2.1. Reglas Generales y Cuestiones Preliminares: *Previo a la práctica de la diligencia procesal, las Fuerzas Policiales y de Seguridad deberán realizar investigaciones preliminares a fin de identificar la dirección IP, números de teléfonos celulares de los dispositivos electrónicos que se utilicen para la comisión del delito denunciado y, principalmente, al supuesto autor del delito objeto de la investigación.*

Identificado el presunto autor, se procurará practicar el allanamiento previendo la presencia del mismo en el lugar, para así poder practicar requisas y secuestro de los elementos que éste tenga encima, siempre y cuando la orden del juez lo contemple.

2.2. Procedimiento: *El allanamiento debe ser practicado de acuerdo a lo establecido en el Código Procesal Penal de la Nación, los Códigos Procesales correspondientes a cada una de las provincias y la CIUDAD AUTÓNOMA DE BUENOS AIRES.*

Una vez dentro del lugar objeto del allanamiento, los agentes deberán visualizar la escena y fotografiar el estado en el que se encuentra, dándole especial relevancia a los dispositivos electrónicos que estén a la vista y cualquier otra anotación que pudiera resultar útil al momento de analizar la evidencia recolectada en el lugar. Deberán reconocer e identificar todos los dispositivos que se encuentran en la escena. Realizado esto, deberán documentar toda la escena especificando el lugar exacto donde se encontraron los dispositivos, el estado en el que se encontraron y el tipo de dispositivo por la relevancia que éstos datos tendrán al momento de reconstruir la escena y se haga la extracción de la prueba digital.

Se deberá poner especial atención en intentar determinar quién o quiénes son los usuarios de los dispositivos.

El personal que manipule la evidencia digital deberá estar especialmente capacitado y entrenado para dicho propósito y deberá utilizar para la recolección guantes de látex, cajas de cartón y bolsas de papel o plásticas según corresponda, debidamente selladas para la recolección de los objetos secuestrados. De esta manera, se evita la contaminación de la posible prueba biológica (ADN, huellas digitales en teclados, mouse etc.) que pueda encontrarse en dichos dispositivos.

Es importante que se registre la marca, modelo y números de serie, así como también cualquier otro tipo de dato de identificación de la computadora y demás dispositivos encontrados en la escena.

2.3 Objetos Susceptibles de Secuestro:

a. Computadoras: Gabinetes, motherboards, microprocesadores, discos rígidos, tarjetas de memoria, laptops, baterías.

b. Dispositivos periféricos: Hardware que puede ser conectado a una computadora para mejorar y expandir las funciones de la máquina: Monitores, teclados, parlantes, discos externos, mouse, módems, routers, impresoras, escáners, faxes, micrófonos. Estos son importantes dados que contienen pruebas biológicas (ADN, huellas digitales…), así como también documentos recientemente escaneados, números entrantes y salientes de fax.

c. Dispositivos de almacenamiento de datos: Disquetes, CD, DVD, Pendrives (pueden estar conectados a la computadora, venir en diferentes tamaños y formas, estar disfrazados u ocultos dentro de otros objetos), Tarjetas de memoria, Micro SD, Discos rígidos, Discos externos.

d. Dispositivos de mano: Celulares, smartphones, tablets, GPS, videocámaras, equipos de vigilancia, consolas de video juegos.

e. Cualquier otro dispositivo que pueda ser susceptible de contener evidencia digital. Potencial prueba que pueden contener: Documentos, imágenes, fotos, emails, bases de datos, información financiera, historial de navegación, log de los chats, discos externos, geo localización.

2.4. Pautas Generales

Los agentes que actúen en el allanamiento deberán:

a. Fotografiar el estado en el que se encuentra el dispositivo y documentar, el estado en el que se lo encontró y el estado en el que se secuestra en caso que haya habido un cambio en la pantalla del dispositivo.

b. Documentar, fotografiar y hacer un esquema de todos los cables y otros dispositivos que estén conectados a la computadora

c. Desconectar y etiquetar el cable de suministro y los demás cables, alambres o dispositivos USB conectados a la computadora.

d. No encender nunca un equipo apagado y si está encendido no apagarlo inmediatamente para evitar la pérdida de información volátil, dependiendo si es necesario para el caso realizar la adquisición de memoria volátil en el lugar del hecho.

e. No desconectar el equipo si el mismo es una estación de trabajo o servidor (conectado en red) o está en un negocio. El desconectarla puede acarrear daño permanente al equipo. Anotar los números de conexión IP y consultar con un técnico experto en redes.

f. Documentar la existencia de cámaras web y si éstas se encuentran activas.

g. Cuando se tengan dudas acerca de si un dispositivo electrónico se encuentra encendido o apagado, mirar y escuchar si existe algún sonido o luz que indique que se encuentra encendido, como ser el ruido de los ventiladores, o las luces led del gabinete si se trata de una computadora.

h. Verificar lo que muestra la pantalla del dispositivo para detectar si se está accediendo a ella remotamente o bien si la información en ella está siendo destruida. Buscar palabras claves tales como borrando, moviendo, limpiando.

i. Buscar señales de actividad de comunicación con otro dispositivo o usuarios a través de ventanas emergentes de chats, de mensajería instantánea, etc.

2.5. Procedimientos especiales

a. Computadora de Escritorio

1. Si el monitor está prendido sacarle una fotografía a la pantalla y anotar la información que se ve.

2. Si el monitor está prendido pero se ve el protector de pantalla, mover ligeramente el mouse sin tocar ningún botón ni mover la rueda. Fotografiar el estado en el que se encontró, anotando y fotografiando lo que aparece posteriormente.

3. Si el monitor está apagado pero el gabinete está encendido, prender el monitor, fotografiar la pantalla y registrar la información que aparezca.

4. Si el monitor está prendido pero la pantalla está en blanco como si estuviese apagada, mover ligeramente el mouse sin tocar ningún botón ni mover la rueda. En el caso que aparezca la pantalla, anotar el cambio de la pantalla, registrar la información y fotografiar el antes y después. Si la pantalla no aparece, confirmar que el gabinete se encuentre encendido, de lo contrario la computadora está apagada. Fotografiar y de ser posible, filmar la escena y documentar el estado en el que se encuentra.

b. Laptop o computadora portátil: Remover el cable de alimentación, localice y remueva la batería, la cual por lo general se localiza debajo del equipo. Seguir los mismos pasos que si se trata de una computadora de escritorio.

c. Dispositivos móviles y celulares:

1. Si el aparato está encendido, no lo apague. Si el aparato está apagado, déjelo apagado.

2. Si lo apaga puede iniciarse el bloqueo del aparato. Transcribir toda la información que aparece en la pantalla y fotografiar el estado en el que se encontró y lo que apareció luego en la pantalla.

3. Revisar los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como Tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2.6. Embalaje, Transporte y Almacenamiento

a. Embalaje: Tener en cuenta que la prueba digital es frágil y sensible a altas temperaturas, humedad, electricidad estática y campos magnéticos.

1. Embalar toda la evidencia digital en bolsas antiestáticas. Solo utilizar bolsas de papel, sobres o cajas de cartón. No deben utilizarse materiales plásticos ya que pueden producir electricidad estática, lo que hace que penetre la humedad.

2. Todo lo que pertenezca a una misma computadora será identificado (etiquetado), embalado y transportado en su conjunto, para evitar que se mezcle con las partes de otros dispositivos y poder luego reconfigurar el sistema.

3. Fajar con fajas de papel y pegamento los puertos y todas las entradas. Sellar cada entrada o puerto de información, tornillos del sistema de manera que no se puedan remover o reemplazar las piezas internas del mismo con cinta de evidencia. Asegurarse que las bandejas de CD o DVD estén cerradas y anotar si estaban vacías o no y fajarlos con cinta adhesiva.

4. Desconectar el cable de suministro.

5. Guardar las baterías de forma separada al equipo.

6. Embalar toda la evidencia teniendo cuidado de no dañar ni alterar nada durante el transporte y almacenamiento.

b. Transporte: Documentar quiénes participaron del empaquetamiento y transporte para registrar la cadena de custodia. Mantener la prueba alejada de campos magnéticos como transmisores de radios, parlantes. Evitar mantener la prueba por tiempo prolongado en el vehículo que la transporte

c. Almacenamiento:

1. Inventariar correctamente toda la prueba.

2. Almacenarla en un ambiente seguro y con un clima controlado para evitar altas temperaturas y humedad.

3. Asegurarse que no esté expuesta a campos magnéticos, humedad, polvo, vibración u otros elementos que puedan dañarla o destruirla.

4. Si se secuestró más de una computadora, almacenar cada una con sus respectivos cables y dispositivos electrónicos por separado.

3. Extracción de la Prueba

Una parte es extraída mediante procedimientos forenses de la propia terminal de la víctima y de los elementos secuestrados.

Otra es facilitada por los proveedores del servicio de Internet, quienes son depositarios de la mayoría de los datos de tráfico válidos para la investigación. Para poder acceder a esta información se requiere de una autorización judicial.

No se debe trabajar con la prueba original si no realizar una copia forense del dispositivo.

En el caso de trabajar con computadoras, se debe realizar primero una copia del disco duro, y luego precintarlo debidamente.

La copia forense puede realizarse por medio de un copiador de hardware o un software. Es obligatorio para este procedimiento:

a. Utilizar un bloqueador de escritura al momento de realizar la copia forense ya que este dispositivo permite operar la computadora asegurando que no se modifique absolutamente la más mínima información, por ejemplo, nos restringirá la mera lectura y copiado de los archivos.

b. Por otro lado, una vez finalizado el copiado, el agente debe realizar el cálculo hash de dicha copia forense.

***3.1. Procedimiento**: Se recomienda hacer dos copias por cualquier eventualidad. Asegurarse que la copia es exacta al original y que durante el proceso del mismo el original permanezca inalterado.*

Obtener un código (hash) que identifique al disco y corroborar que el mismo sea igual al código de la copia. Por lo tanto, ante el mínimo cambio tanto en el original como en la copia, se daría como resultado un código distinto.

3.2. Potencial Prueba Extraíble:

a. Registros de chats y blogs

b. Software de reproducción, captura y edición de video

c. Imágenes y videos de contenido sexual

d. Juegos infantiles o de contenido sexual

e. Registros de actividad en internet

f. Directorios de archivos encriptados o no visibles mediante los cuales clasifica el contenido de las distintas víctimas.

g. Correos electrónicos, notas y cartas varias

h. Papeles con contraseñas anotadas, notas, manuales de hardware y software, calendarios, material pornográfico, DVD, CD, Disquetes, etc.

***3.3. Cadena de Custodia**. La cadena de custodia debe contener:*

a. Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, identificación del encargado de custodia, identificaciones, cargo, y firmas de quien recibe y quien entrega.

b. Rótulos que van pegados a los envases de la prueba.

c. Etiquetas con la misma información de los rótulos que van atadas con cuerda al paquete de la prueba que corresponda.

d. Libros de registros de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios.

4. Capacitaciones

El MINISTERIO DE SEGURIDAD se compromete a realizar capacitaciones para los agentes de la POLICÍA FEDERAL ARGENTINA, GENDARMERÍA NACIONAL, PREFECTURA NAVAL, Y POLICÍA DE SEGURIDAD AEROPORTUARIA en temas vinculados a los ciberdelitos y la investigación y prevención de los mismos, mediante el dictado de cursos, talleres y seminarios diseñados a tal fin.

El contenido y programa de las capacitaciones versará sobre definiciones, lineamientos, protocolos de actuación, herramientas de investigación de los delitos y tratamiento de las víctimas. Dicho contenido será establecido por el Ministerio.

Unidad 3

> Cadena de custodia

U3

La cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de los objetos o muestras que pueden ser fuente de prueba de hechos criminales (preservación total de su eficacia procesal).

La documentación de dicha actividad a partir de la planilla correspondiente, permite detallar las particularidades de los elementos materia de prueba, los custodios, el lugar, el sitio exacto, fecha y hora de los traspasos y traslados de los mismos.

Objetivos de la cadena de custodia

1. Unificar los criterios de funcionamiento del sistema de cadena de custodia mediante la estandarización de los procedimientos de trabajo.

2. Describir los lineamientos básicos para el desarrollo del sistema de cadena de custodia, mejorando el desempeño y confiabilidad de quienes tengan contacto con los elementos materia de prueba o evidencias físicas.

3. Normalizar y estandarizar la ejecución del trabajo en el manejo del sistema de cadena de custodia.

4. Garantizar que el elemento de prueba o evidencia que se presenta finalmente en juicio, con el objeto de probar una determinada afirmación, sea el elemento que ha sido levantado o reclutado y, que no haya sufrido adulteraciones o modificaciones de parte de quienes lo introducen, o terceras personas.

5. Evitar cuestionamientos respecto del levantamiento y custodia de los elementos o rastros que se presentan en juicio, desterrando cualquier sospecha sobre su procedencia y dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen, o cualquier otra diligencia procesal (ej.: allanamiento).

Reglas de obligatoriedad general

“Toda evidencia o elemento materia de prueba que se ingrese a la Oficina de Efectos Departamental, deberá estar acompañado de: la Planilla de Cadena de Custodia, copia del acta de procedimiento y/o allanamiento, secuestro y copia del informe de visu (éste último, en caso de corresponder)”,

“Toda evidencia o elemento materia de prueba se traslada de un lugar a otro (ej.: sala de efectos hasta laboratorio para pericia) con su Planilla de Cadena de Custodia y con todas las actas de apertura a las que diere lugar”.

Aspectos relevantes sobre la documentación.

(Planilla de cadena de custodia)

1. La Planilla de Cadena de Custodia y la documentación originada en la aplicación del presente sistema, deberán estar exentas de modificaciones o alteraciones por raspado, borrado, lavado, agregados, tachadura, enmienda, retoque o cualquier otro hecho que atente contra el principio de integridad.

2. En caso de recibirse los elementos en mal estado o con alguna irregularidad, deberá dejarse asentada dicha circunstancia en la Planilla de Cadena de Custodia.

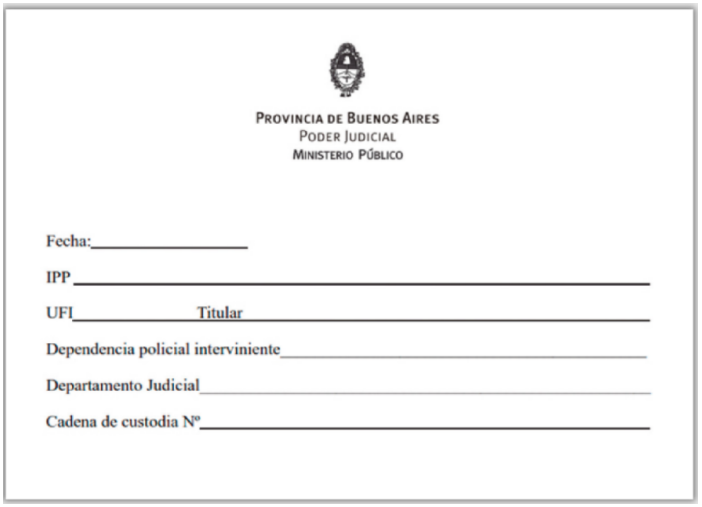
3. El registro de la cadena de custodia debe diligenciarse en un solo ejemplar original SIN COPIAS.

4. Quien reciba las muestras deberá diligenciar el registro de continuidad de cadena de custodia en presencia de quien entrega.

5. Cuando la Planilla de Cadena de Custodia no sea suficiente para el registro de continuidad de las muestras, se podrá utilizar hojas adicionales cuantas sean necesarias, y se deberá anotar en la parte superior derecha de cada hoja el número que corresponde del total de hojas utilizadas.

Nota: el formato de la Planilla de Cadena de Custodia en sus diversas versiones (drogas, elementos informáticos y demás muestras) se encuentra disponible en la página web: www. mpba.gov.ar. en el link correspondiente a la Secretaría de Política Criminal.

Modelo de faja



PROVINCIA DE BUENOS AIRES
PODER JUDICIAL
MINISTERIO PÚBLICO

Fecha:_____

IPP_____

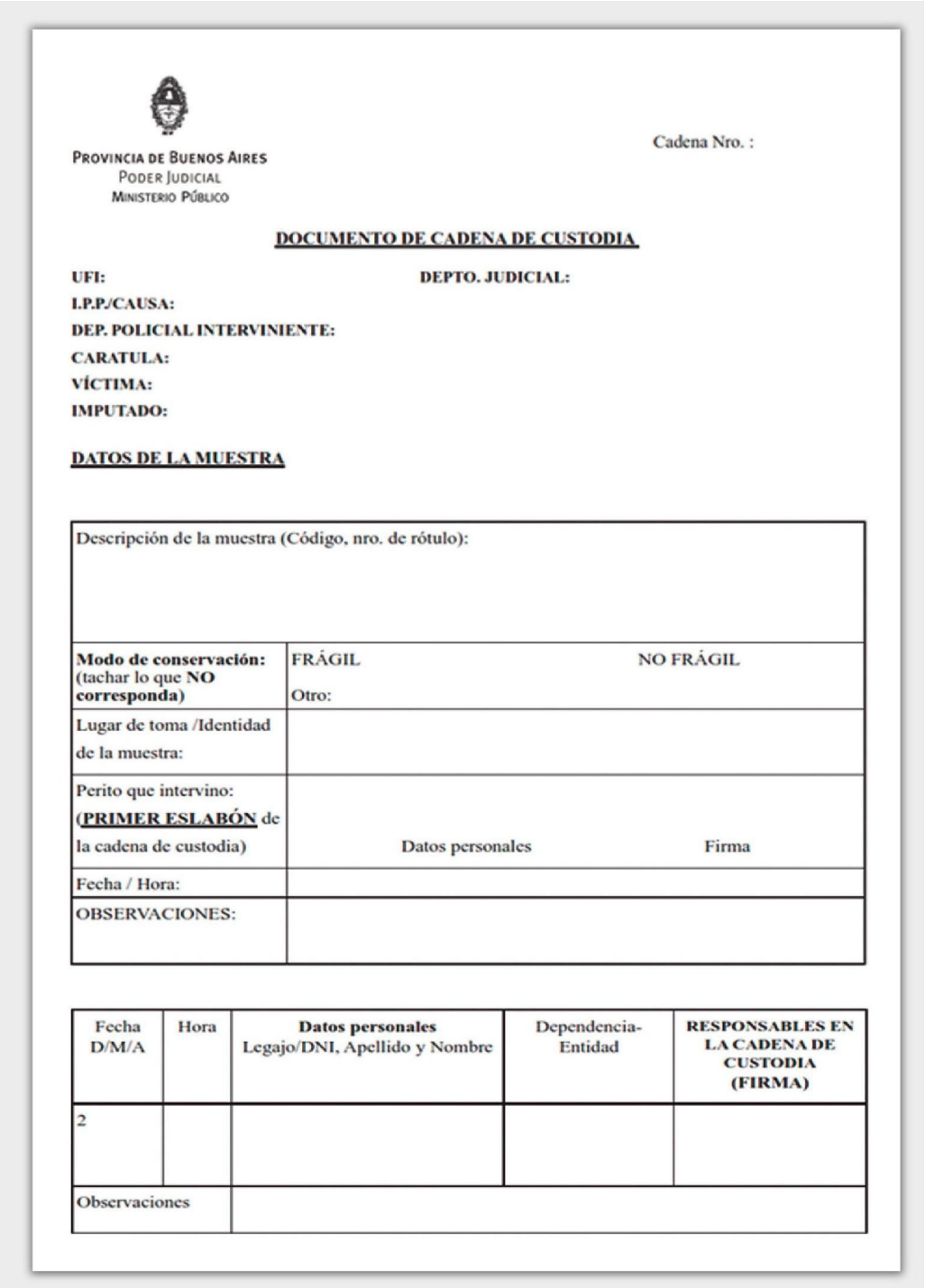
UFI_____ Titular_____

Dependencia policial interviniente_____

Departamento Judicial_____

Cadena de custodia Nº_____

Modelo de acta



PROVINCIA DE BUENOS AIRES
PODER JUDICIAL
MINISTERIO PÚBLICO

Cadena Nro. :

DOCUMENTO DE CADENA DE CUSTODIA

UFI: **DEPTO. JUDICIAL:**
I.P.P./CAUSA:
DEP. POLICIAL INTERVINIENTE:
CARATULA:
VÍCTIMA:
IMPUTADO:

DATOS DE LA MUESTRA

Descripción de la muestra (Código, nro. de rótulo):		
Modo de conservación: (tachar lo que **NO corresponda)**	FRÁGIL Otro:	NO FRÁGIL
Lugar de toma /Identidad de la muestra:		
Perito que intervino: (**PRIMER ESLABÓN** de la cadena de custodia)	Datos personales	Firma
Fecha / Hora:		
OBSERVACIONES:		

Fecha D/M/A	Hora	**Datos personales** Legajo/DNI, Apellido y Nombre	Dependencia-Entidad	**RESPONSABLES EN LA CADENA DE CUSTODIA (FIRMA)**
2				
Observaciones				

Resolución 234/16

Resolución 234/16

La Plata, 9 de octubre de 2015.

VISTO:

Los artículos 18 de la Constitución Nacional, 16 de la Constitución Provincial, 248, 266,

294, 342 bis del C.P.P., y 29 inc. 2 de la Ley nro. 14.442;

Y CONSIDERANDO:

Que en materia de preservación de los medios de prueba, ha resultado imperioso la construcción desde la órbita de esta Procuración General, de un mecanismo de legalidad que permita afianzar la garantía del debido proceso penal, por un lado, e implementar un conjunto de medidas con la finalidad de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba en hechos criminales, por el otro.

Que en esa inteligencia, la documentación de la actividad investigativa desarrollada a partir de la creación e implementación de una planilla de cadena de custodia -en la cual se detallen las particularidades de los elementos materia de prueba, los custodios, el lugar, el sitio o ubicación exactos, fecha y hora de los traspasos y traslados de los mismos-, nos permite arribar a la conclusión que, hoy en día, la cadena de custodia es más que un documento: es la realidad misma de la confianza que debe ofrecer toda evidencia o indicio de prueba.

Que sobre este aspecto, no podemos soslayar que la "evidencia" es parte fundamental, no sólo de la parte inicial de la investigación criminal, sino más bien, de todo el proceso penal acusatorio, habida cuenta que será a través de ésta y de su legitimación, que se logrará el convencimiento en el ánimo del juzgador; siempre y cuando, por supuesto, dicho proceso investigativo se haya sujetado al cumplimiento de los pasos ordinarios que se refieren al registro inicial de la ubicación del indicio en sí, a su detallada y precisa descripción, marcaje numerado, fijación fotográfica, embalaje y etiquetado correspondientes, así como su posterior traslado y correcto llenado de los documentos o formatos legales que amparen tales acciones, vinculándolas con las personas involucradas en ello; procedimientos que en conjunto constituyen un requisito indispensable para el debido cumplimiento de la cadena de custodia.

Que en este sentido, debemos recordar que, algunos magistrados (particularmente, en la etapa de celebración del juicio oral), han rechazado y declarado nula la prueba aportada

-no por cuestiones vinculadas a la prueba en sí misma-, sino en fundamento a la ausencia, irregularidad, desprolijidad o visos de alteración en la cadena de custodia.

Que en mérito a ello, bajo la supervisión y coordinación de la Secretaría de Política Criminal, Coordinación Fiscal e Instrucción Penal, se procedió a la elaboración de un "Protocolo de Cadena de Custodia", a los fines de: unificar los criterios de funcionamiento del sistema de cadena de custodia mediante la estandarización de los procedimientos de trabajo; describir los lineamientos básicos para el desarrollo del sistema de cadena de custodia, mejorando el desempeño y confiabilidad de quienes tengan contacto con los elementos materia de prueba o evidencias físicas; normalizar y estandarizar la ejecución del trabajo; y finalmente, garantizar que el elemento de prueba o evidencia que se presenta finalmente en juicio, con el objeto de probar una determinada afirmación, sea el elemento que ha sido levantado o reclutado y que no ha sufrido adulteraciones o modificaciones de parte de quienes lo introdujeron, o terceras personas.

Que por todo lo expuesto, el "Protocolo de Cadena de Custodia" resulta ser una herramienta de consulta ágil y de apoyo para el operador judicial, encontrándose sujeto a todas aquellas modificaciones que, como consecuencia del carácter dinámico de los delitos y el devenir de la práctica judicial, resulten menester.

***POR ELLO**:*

La Señora Procuradora General ante la Suprema Corte de Justicia de la Provincia de Buenos Aires, en uso de sus atribuciones (art. 189, último párrafo de la Constitución de la provincia de Buenos Aires y arts. 1, 2,20 Y 21 de la Ley 14442

Resuelve

***Artículo 1°:** REQUERIR a los Señores Fiscales Generales Departamentales que, instruyan a los agentes fiscales a que observen y apliquen el "Protocolo de Cadena de Custodia", que como anexo I se añade a la presente.*

***Artículo 2°:** Regístrese, comuníquese.*

REGISTRADO BAJO EL N° 889\ 5 Procuración General

ANEXO I

PROTOCOLO DE CADENA DE CUSTODIA

***Cadena de Custodia**: La cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de los objetos o muestras que pueden ser fuente de prueba de hechos criminales (preservación total de su eficacia procesal). La documentación de dicha actividad a partir de la planilla correspondiente, permite detallar las*

particularidades de los elementos materia de prueba, los custodios, el lugar, el sitio exacto, fecha y hora de los traspasos y traslados de los mismos.

Objetivos:

1. Unificar los criterios de funcionamiento del sistema de cadena de custodia mediante la estandarización de los procedimientos de trabajo.

2. Describir los lineamientos básicos para el desarrollo del sistema de cadena de custodia, mejorando el desempeño y confiabilidad de quienes tengan contacto con los elementos materia de prueba o evidencias físicas.

3. Normalizar y estandarizar la ejecución del trabajo en el manejo del sistema de cadena de custodia.

4. Garantizar que el elemento de prueba o evidencia que se presenta finalmente en juicio, con el objeto de probar una determinada afirmación, sea el elemento que ha sido levantado o reclutado y, que no haya sufrido adulteraciones o modificaciones de parte de quienes lo introducen, o terceras personas.

5. Evitar cuestionamientos respecto del levantamiento y custodia de los elementos o rastros que se presentan en juicio, desterrando cualquier sospecha sobre su procedencia y dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen, o cualquier otra diligencia procesal (ej.: allanamiento).

Reglas de obligatoriedad general:

"Toda evidencia o elemento materia de prueba que se ingrese a la Oficina de Efectos Departamental, deberá estar acompañado de: la Planilla de Cadena de Custodia, copia del acta de procedimiento y/o allanamiento y secuestro y copia del informe de visu (éste último, en caso de corresponder)",

"Toda evidencia o elemento materia de prueba se traslada de un lugar a otro (ej.: sala de efectos hasta laboratorio para pericia) con su Planilla de Cadena de Custodia y con todas las actas de apertura a las que diere lugar".

Aspectos relevantes sobre la documentación (Planilla de Cadena de Custodia):

1. La Planilla de Cadena de Custodia y la documentación originada en la aplicación del presente sistema, deberán estar exentas de modificaciones o alteraciones por raspado, borrado, lavado, agregados, tachadura, enmienda, retoque o cualquier otro hecho que atente contra el principio de integridad.

2. En caso de recibirse los elementos en mal estado o con alguna irregularidad, deberá dejarse asentada dicha circunstancia en la Planilla de Cadena de Custodia.

3. El registro de la cadena de custodia debe diligenciarse en un solo ejemplar original SIN COPIAS.

4. Quien reciba las muestras deberá diligenciar el registro de continuidad de cadena de custodia en presencia de quien entrega.

5. Cuando la Planilla de Cadena de Custodia no sea suficiente para el registro de continuidad de las muestras, se podrá utilizar hojas adicionales cuantas sean necesarias, y se deberá anotar en la parte superior derecha de cada hoja el número que corresponde del total de hojas utilizadas.

Nota: el formato de la Planilla de Cadena de Custodia en sus diversas versiones (drogas, elementos informáticos y demás muestras) se encuentra disponible en la página web: www.mpba. gov.ar. en el link correspondiente a la Secretaría de Política Criminal.

Guía de actuación en el sistema de Cadena de Custodia:

1. Previa fijación -la recolección, embalaje y rotulación de los elementos materia de prueba o evidencia-, la documentación de las muestras en la Planilla de Cadena de Custodia se realizará teniendo en cuenta la clase, naturaleza y estado de las mismas, separando las muestras de acuerdo a la "familia de efectos" (ej.: dinero, armas, ropas, etc.).

2. Consecuentemente, existirán tantas Planillas de Cadena de Custodia por cada familia de efectos que se genere.

3. La Planilla de Cadena de Custodia acompañará a las muestras desde la recolección hasta su disposición final.

4. El funcionario judicial o de prevención que hubiere recogido, embalado y rotulado los elementos de prueba o evidencia, deberá hacer el traspaso de los mismos con la Planilla de Cadena de Custodia pertinente, ya sea que aquéllos se trasladen a la Oficina de Efectos Departamental o al Laboratorio que correspondiera.

5. Toda persona que deba recibir un elemento material probatorio o evidencia física, antes de hacerlo, revisará el recipiente que lo contiene (sobre, bolsa, etc.). En principio, el embalaje sólo se podrá abrir por el perito designado para su estudio y análisis, a excepción que, en los sitios de recepción del elemento (ej.: Oficina de Efectos Departamental, U.F.I.J.) por motivos de seguridad, exista la necesidad de verificar el contenido del embalaje; en cuyo caso se procederá a abrir el contenedor en presencia de un testigo, asentándose dicha circunstancia, en el Acta de Apertura respectiva (ej.: el supuesto de ingreso de armas de fuego para verificar si están descargadas). Dicha Acta de Apertura acompañará a la Planilla de Cadena de Custodia desde el mismo momento en que fue creada, y cualquiera sea el lugar de origen. Asimismo, la apertura del contenedor se hará por el lado diferente a donde se encuentre el sello inicial. Despejada la duda, el elemento se introducirá preferentemente en el

embalaje inicial (si las condiciones del mismo lo permiten). En caso de utilizarse un nuevo embalaje, se conservará el rótulo y sello inicial.

6. Al momento de realizarse el traspaso del elemento material probatorio o evidencia a la persona encargada de su transporte (ej.: oficial de policía que actuará como correo), deberá dejar constancia -tanto de la recepción del elemento como de la entrega- en la Planilla de Cadena de Custodia respectiva.

7. Ningún personal recepcionará elemento o muestra materia de prueba o evidencia física que no esté embalado, sellado, rotulado y con el registro de la Planilla de Cadena de Custodia, a excepción que exista imposibilidad para ello, en cuyo caso, con la presencia de un testigo se hará uso de los medios más adecuados para tal fin garantizando siempre el principio de autenticidad (ej.: cuando por razones de urgencia y seguridad personal, las circunstancias tornaron peligroso la permanencia del personal en el lugar del hecho).

8. Cuando las muestras tomadas no guarden correspondencia con el número total de los elementos materia de prueba o evidencias físicas descriptos en el acta de procedimiento correspondiente, el funcionario dejará constancia de ello en el ítem "observaciones" e iniciará un nuevo registro de Cadena de Custodia para las muestras que fueron omitidas.

Guía de actuación para el registro de la cadena de custodia en elementos informáticos y telefonía celular

La cadena de custodia informático forense es un procedimiento controlado que se aplica a los indicios materiales o virtuales. La prueba documental informática consiste en indicios digitalizados, codificados y resguardados en un contenedor digital específico. Es decir, toda información es información almacenada (aún durante su desplazamiento por una red).

Para que la prueba documental informática sea tenida por válida y adquiera fuerza probatoria, es necesario que la misma sea garantizada respecto de su confiabilidad, evitando suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente, su destrucción (algo muy común en la evidencia digital).

Nota: Es necesario diferenciar entre el objeto que contiene a la información (discos magnéticos, ópticos, etc.) de su contenido: información almacenada y, muy particularmente, de su significado.

Recolección de evidencia:

1. Es crucial la manera en que se recopila y preserva la evidencia electrónica para cualquier investigación. Siempre que sea posible, un forense informático debe ser consultado con anterioridad al allanamiento y/o cualquier medida procesal dispuesta.

2. Los medios digitales son sumamente volátiles, por lo tanto, su sola consulta y toma de vista, crea un impacto en el tiempo. Para preservar la prueba (en el punto utilizado por última vez), es imprescindible contar con el dispositivo apagado, el cable de alimentación se retira y se debe almacenar impidiendo el acceso a todo tipo de conector y botón de encendido; de manera tal de garantizar la integridad física de cada dispositivo.

3. Impedir por los medios que sean necesarios, que los dispositivos sean manipulados por personas que no estén capacitadas para realizar la tarea de análisis.

4. Toda la información pertinente a la investigación, debe ser obtenida con anterioridad a cualquier trabajo o manipulación que se vaya a realizar sobre los datos contenidos en los dispositivos electrónicos, esto incluye: las contraseñas de acceso a redes y aplicaciones que las requieran, identificar tipo de sistema operativo utilizado, direcciones de correo electrónico, software de interés o cualquier otro dato específico.

5. Es siempre importante fotografiar sistemáticamente todo el espacio de trabajo y buscar dispositivos o señales de su uso y de almacenamiento de datos alternativos (los discos duros externos, disquetes, unidades de memoria flash, tarjetas de memoria, grabadoras de voz, cámaras digitales, ipods o cualquier tipo de reproductor, consolas de video juegos, etc.). Del mismo modo, fotografiar cada dispositivo graficando, en lo posible, la fecha y hora del mismo. Ej.: fotografiar la pantalla del monitor encendido del equipo dubitado, las vistas frontal, lateral y posterior (según corresponda), números de serie, etiquetas de garantía; periféricos (teclados, mouse, impresoras, agendas PDA, videocámaras, video grabadora, pendrive, dispositivos de almacenamiento en red, unidades de zip o jazz, celulares, ipods, entre otros).

6. La documentación de la recolección de cualquier dispositivo electrónico debe especificar y detallar, muy particularmente, la ubicación geográfica del mismo identificando (con al menos, una letra y un número) cada uno de los elementos informáticos, como así también, del total.

7. En el supuesto de secuestrarse CPUs, se debe colocar una faja de seguridad obstaculizando los sectores de entrada, PEGADA con algún elemento adhesivo (ej.: plasticola), SIN CINTA Y procurando que la faja no esté arrugada. Finalmente, el elemento informático debe ser colocado dentro de una caja de cartón.

Nota: la faja de seguridad puede obtenerse de la página web: www.mpba.gov.ar. en el link correspondiente a la Secretaría de Política Criminal.

8. El procedimiento óptimo para el traslado de los elementos informáticos es la utilización de cajas de cartón, evitando que los medios electrónicos se encuentren sueltos dentro de las mismas. Toda la información identificatoria del elemento secuestrado, debe

estar estampada directamente sobre el contenedor (caja), de la manera más legible posible; detallándose principalmente, si el elemento es "frágil" o "no frágil".

9. Debe realizarse UNA PLANILLA de Cadena de Custodia POR CADA MÁQUINA SECUESTRADA, ya que la faja está relacionada con el registro correspondiente de su cadena de custodia.

10. Tener presente, particularmente en los casos de pornografía infantil, el detalle exhaustivo en el acta de procedimiento, del lugar de donde se secuestró el CPU (ej.: dormitorio, living, etc.).

11. En el secuestro de teléfonos celulares: apagarlos y, posteriormente, desarmarlos prolijamente para ser entregados con su correspondiente Planilla de Cadena de Custodia, acta de procedimiento e informe de visu, a la oficina pericial o de efectos departamental.

12. Documento logia: incluye CD de escuchas, filmaciones, etc. Cada documento (ej.: historia clínica), como Cds., deben llevar también la Planilla de Cadena de Custodia correspondiente.

Resulta óptimo que la documentación no se encuentre glosada en la causa. Sino más bien, que sea remitida con su correspondiente Planilla de Cadena de Custodia a la Oficina de Efectos Departamental, dejándose expresa constancia en la I, P.P.

- Asesoramiento/Asistencia a la Víctima.
- Consultas.

Programa Línea 102

Línea 102

Es un servicio telefónico gratuito que brinda la Secretaría de Niñez y Adolscencia, de orientación sobre la garantía y restitución de los derechos de la infancia en la provincia de Buenos Aires. Funciona las 24 horas, los 365 días del año.

Equipos niñ@s contra la explotación sexual y grooming

Línea 0800-222-1717

Es un servicio telefónico gratuito del Ministerio de Justicia y Derechos Humanos las 24 horas, los 365 días del año, en toda Argentina. También por mail a equiponinas@jus.gov.ar

Mapa de las Fiscalías por Departamento Judicial de la Procuración General de la Provincia de Bs. As.

www.mpba.gov.ar

Dirección Provincial del Centro de Protección de los Derechos de las Víctimas

0800-666-4403
0221-489-8610 / 8666

Referencias

Normativa

- Ley 26.388 de 2008. Código Penal. B.O. del 25 de junio de 2008. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

- Ley 27.411 de 2017. Convenio sobre ciberdelito del consejo de Europa. B.O del 15 de diciembre de 2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm

- Ley 26.904 de 2013. Incorporación del artículo 131 al código penal por delito de Grooming. B.O del 11 de diciembre de 2013. http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

- Ley 27.436 de 2018. Modificación del Código Penal. B.O del 23 de abril de 2018. http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/309201/norma.htm

- Ley 26.842 de 2012. Prevención y sanción de la trata de personas y asistencia a sus víctimas. B.O del 27 de diciembre de 2012. http://servicios.infoleg.gob.ar/infolegInternet/anexos/205000-209999/206554/norma.htm

- Resolución 234/2016. Protocolo general en la investigación y proceso de recolección de pruebas en ciberdelitos. B.O del 14 de junio de 2016. http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm