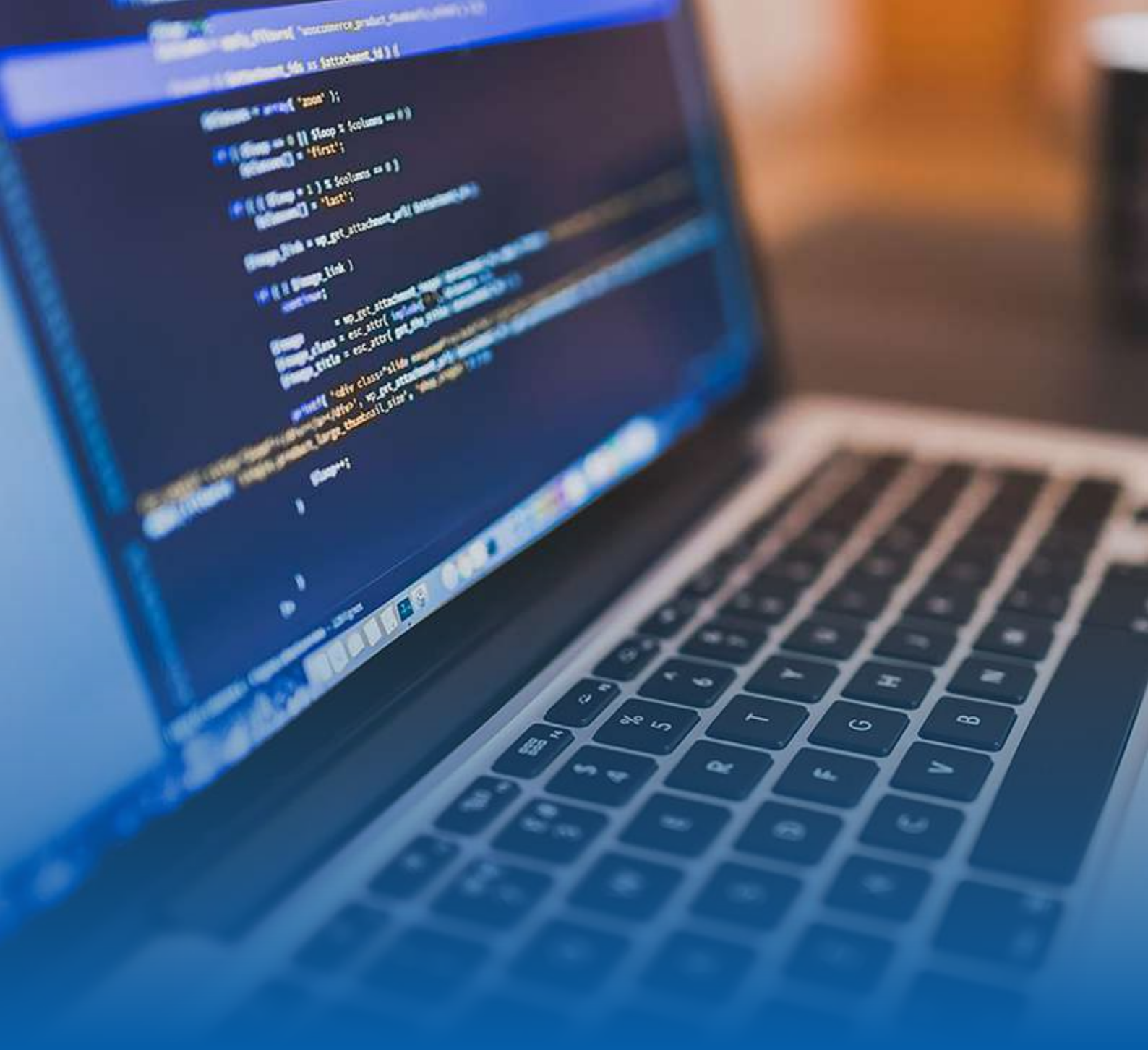


SEGEN

DELITOS CIBERNÉTICOS
NOCIONES BÁSICAS

PRESIDÊNCIA DA REPÚBLICA
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
SECRETARIA DE GESTÃO E ENSINO EM SEGURANÇA PÚBLICA

Conteudistas
André Santos Guimarães
Ricardo Magno Teixeira Fonseca.

Revisão Pedagógica
Anne Caroline Bogarin Manzolli
Ardmon dos Santos Barbosa
Márcio Raphael Nascimento Maia

UNIVERSIDADE FEDERAL DE SANTA CATARINA
SECRETARIA DE EDUCAÇÃO A DISTÂNCIA
labSEAD

Comitê Gestor
Luciano Patrício Souza de Castro

Financeiro
Fernando Machado Wolf

Consultoria Técnica EaD
Giovana Schuelter

Coordenação de Produção
Francielli Schuelter

Coordenação de AVEA
Andreia Mara Fiala

Design Instrucional
Danrley Maurício Vieira
Marielly Agatha Machado

Design Gráfico
Aline Lima Ramalho
Douglas Wilson Lisboa de Melo
Sonia Trois
Taylizy Kamila Martim

Linguagem e Memória
Cleusa Iracema Pereira Raimundo
Victor Rocha Freire Silva

Tradução
Cristhian Fernando Rondon Mora
Paula Balbis Garcia

Programação
Jonas Batista
Salésio Eduardo Assi
Thiago Assi

Audiovisual
Luiz Felipe Moreira Silva Oliveira
Rafael Poletto Dutra
Rodrigo Humaita Witte

Resumen

Presentación del Curso

Te damos la bienvenida al curso **Delitos Cibernéticos: Nociones Básicas**.

Una de las principales características que marcan la diferencia entre las sociedades tecnológicas y las sociedades antiguas es la conectividad entre países, personas y empresas mediante redes informáticas, especialmente por Internet. En el contexto de este fenómeno, el ciberespacio se ha convertido en un área de intercomunicación social. Debido a esto, se ha desarrollado una asociación entre los mundos real y virtual, condensada hoy en día de tal manera que cada vez es más difícil establecer sus propios límites.

Así pues, ha surgido la preocupación de los países por el avance de las nuevas formas de crímenes Cibernéticos, ya que el entorno virtual es específico y la identificación del lugar del delito y los vestigios por parte de los agentes de seguridad pública deben ser precisos, teniendo en cuenta el sesgo que rodea a la legislación. Por lo tanto, es necesario comprender que la legislación que rige el fenómeno de los delitos electrónicos en el Brasil es bastante reciente en comparación con otras leyes que componen el sistema jurídico brasileño. Por lo tanto, el propósito de este curso es brindar a todos los profesionales de seguridad pública un estudio teórico y técnico sobre el proceso de investigación de crímenes cibernéticos. Para ello, en este curso, conocerás aspectos históricos e instrumentos de lucha contra la delincuencia en los ámbitos nacional y mundial, además de la preservación de la jurisdicción, los protocolos, las normas y los procedimientos del proceso de investigación, materializando el estudio con el conocimiento de un caso concreto de investigación de crímenes electrónicos en Brasil.

¡Te deseamos un excelente estudio!

Equipo del curso.

MÓDULO 1

CIBERESPACIO E INTERNET

Presentación

¿Qué diferencia nuestra etapa de desarrollo social con épocas anteriores?

Una de las principales diferencias es la conectividad entre países, personas y empresas a través de las redes informáticas, especialmente Internet. Este es el fenómeno que constituye la principal nota distintiva de la actual etapa de desarrollo de la sociedad mundial, que repercute en los modelos comerciales tradicionales y le aporta a un nuevo mercado de consumidores productos capaces de cambiar sus hábitos de vida.

El crecimiento de esta red de información es exponencial e irreversible, considerando la migración masiva de los hábitos y rutinas humanas hacia el mundo digital, transformando en general, el modo de vida en el planeta. En este módulo, comprenderemos la historia de esta evolución tecnológica, el concepto de internet y su funcionamiento, así como el estudio de los principales protocolos existentes.

OBJETIVOS DEL MÓDULO

Comprender el origen de la red informática y de Internet, así como sus conceptos y nociones de funcionamiento. Además de eso, conocer los principales protocolos de internet, y conceptualizar Internet, la *Web* y el Ciberespacio.

ESTRUCTURA DEL MÓDULO

- **Clase 1 -** El Origen de las Redes Informáticas.
- **Clase 2 -** Concepto de Internet.
- **Clase 3 -** Nociones sobre el Funcionamiento de Internet.
- **Clase 4 -** Principales Protocolos de Internet.
- **Clase 5 -** El Protocolo IP: Tipos y Características.
- **Clase 6 -** Protocolos HTTP y HTTPS: Internet y la *Web*.
- **Clase 7 -** Concepto y Características del Ciberespacio.

Clase 1 – El Origen de las Redes Informáticas

CONTEXTUALIZANDO...

En esta clase, examinaremos brevemente la historia de una red creada inicialmente para cumplir con estrategias militares, pero desplegada por entusiastas y visionarios del entorno universitario. Revisaremos por una línea histórica para entender la evolución de esta tecnología, a través de los estudios de las décadas de 1960, 1970, 1980 y 1990.

DÉCADA DE 1960

El primer capítulo de esta historia se remonta a los acontecimientos que siguieron al final de la Segunda Guerra Mundial. La Guerra Fría, establecida entonces entre los Estados Unidos y la Unión Soviética, estimuló el desarrollo de tecnologías en armas y en la carrera espacial.

Hasta entonces, la única forma de establecer la comunicación entre dos nodos de una red era mediante la conmutación de circuitos, en la que los recursos de transmisión se reservaban para su uso exclusivo en el circuito durante la conexión. La telefonía era el ejemplo más conocido de este tipo de tecnología.

En este contexto, tres proyectos fueron importantes para la creación de la red informática.

1

En 1957, la Unión Soviética lanzó sus satélites Sputniks. En la década del 60, el Departamento de Defensa de los Estados Unidos presentó al mundo una iniciativa destinada a crear una red informática capaz de comunicar a los usuarios en diferentes lugares.

2

En 1962, bajo la dirección de John Licklider, un científico del Instituto Tecnológico de Massachusetts (MIT), el equipo de investigadores desarrolló un programa de investigación informática, considerado la "piedra angular" en la construcción de la "red galáctica".

3

Simultáneamente, los investigadores Leonard Kleinrock del MIT, Donald Davies del NPL, el Laboratorio de Física del Reino Unido y Paul Baran de la Corporación RAND trabajaron en diferentes proyectos destinados a crear un nuevo método de comunicación segura e informatizada.

Figura 1: Proyectos que dieron origen a la red informática. **Fuente:** labSEAD-UFSC (2020).

Estas iniciativas se desarrollaron en paralelo hasta que, en 1968, el Departamento de Defensa de los Estados Unidos estructuró una agencia llamada Agencia de Proyectos de Investigación Avanzada (Advanced Research Projects Agency - ARPA), implementando, definitivamente, la investigación en tecnologías informáticas en las universidades. ARPA unificó los tres proyectos mencionados anteriormente para implementar una red informática capaz de comunicar diferentes instituciones académicas y estatales.

También podemos citar la importante contribución del Dr. Leonard Kleinrock. Su trabajo en la teoría de colas fue fundamental como base matemática para el cambio de paquetes. Era un método de enviar datos por una red informática a través de paquetes de información. Así, fue posible utilizar diferentes redes para enviar la información de forma secuencial, pero asegurándose de que todos los paquetes llegaran a su destino para obtener el mensaje completo.

Así, a mediados de 1968, ya existía un plan para construir la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET) - y en abril de 1969, Bolt, Beranek y Newman fueron elegidos para implementar esta red instalando **Procesadores de Mensajes de Interfaz** - Interface Message Processors **(IMPs)**. Se trataba de dispositivos dedicados al almacenamiento y reenvío de paquetes de datos, los cuales utilizaban un módem telefónico para conectarse a otros equipos. De esta manera, las computadoras centrales se conectaron a las IMPs a través de una interfaz serial personalizada.

De esta manera, las computadoras principales se conectaron a las IMPs por medio de una interfaz serial personalizada. Inicialmente, ARPANET tenía solo cuatro IMPs como infraestructura, instalados en las siguientes instituciones:

- Universidad de Los Ángeles (UCLA).
- Universidad de Santa Bárbara.
- Instituto de Investigación de Stanford.
- Universidad de Utah.

Finalmente, la primera comunicación a través de ARPANET se realizó el 29 de octubre de 1969 entre la UCLA y el Instituto de Investigación de Stanford.

> El intento considerado histórico, en 1969, se limitó al envío de un mensaje que contenía la palabra *login*, pero en este primer envío solo llegaron dos letras y la conexión falló. Una hora más tarde, fue posible completar el envío. Esta sería la primera vez que un ordenador se conectaría a otro a cientos de kilómetros de distancia.

Dos momentos se consideran importantes para la inauguración completa de la red.

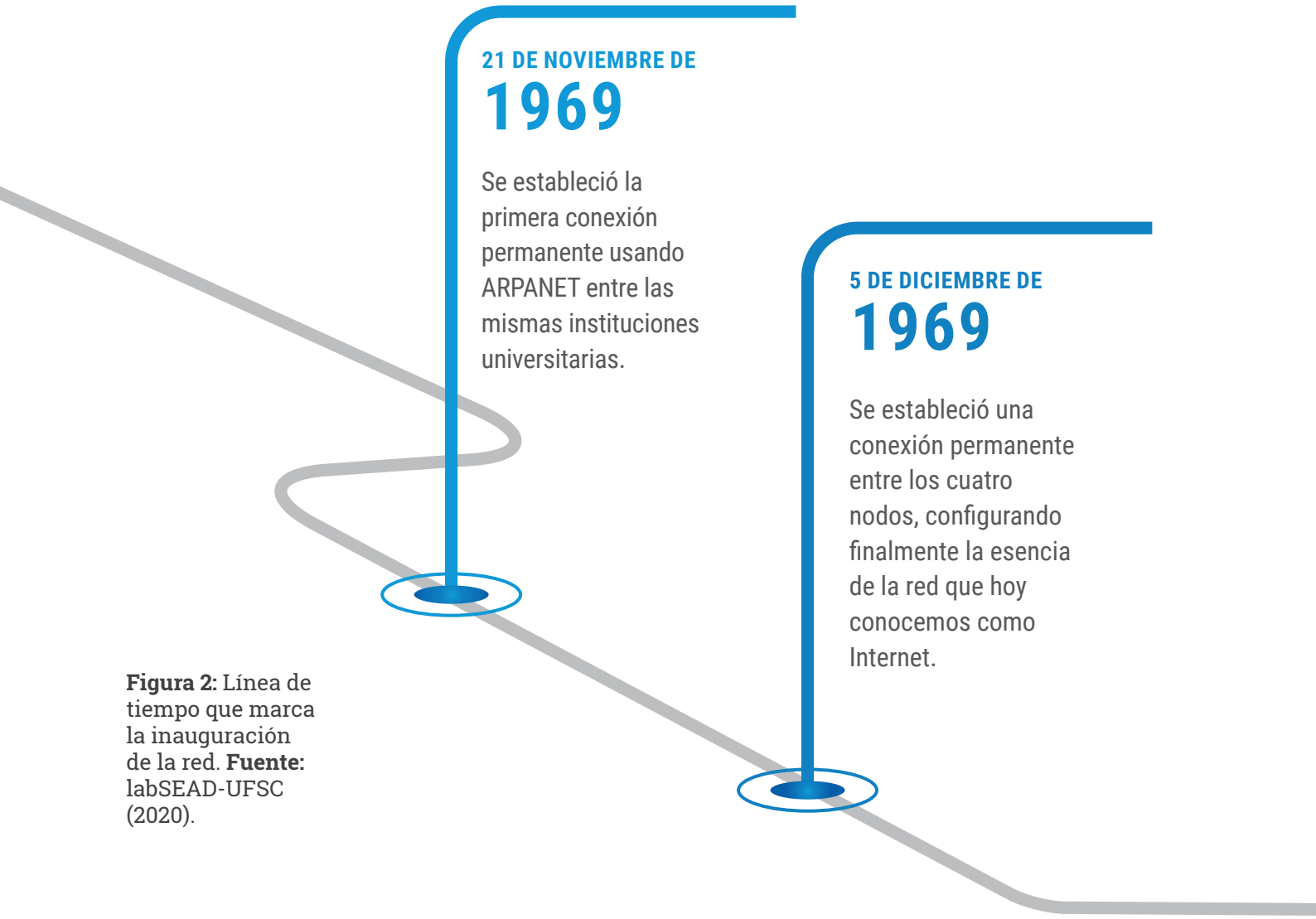


Figura 2: Línea de tiempo que marca la inauguración de la red. **Fuente:** labSEAD-UFSC (2020).

Así comenzó su expansión durante los años siguientes, añadiendo gradualmente más computadoras.

DÉCADA DE 1970

Fue a principios de los años 1970 cuando los conceptos básicos de Internet que se conocen hoy en día fueron establecidos por la Agencia de Desarrollo de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de los Estados Unidos.

> Algunos historiadores señalan que el objetivo del proyecto era crear una red, cuyo funcionamiento fuera menos vulnerable a un ataque atómico y cuyas vías de comunicación fueran menos interceptables. Sin embargo, el potencial transformador de esta creación, en poco tiempo, se vio y sus diseños se ampliaron, lo que requirió una estandarización de los protocolos y una documentación detallada.

En esa década se comenzó a trabajar en una serie de documentos públicos que definen los protocolos, conceptos, métodos y programas de Internet, llamados Request for Comments (RFCs), que pueden ser traducidos como una solicitud de comentarios. Este aspecto fue muy importante y estimulante para el desarrollo de diferentes protocolos y procedimientos de construcción en la red que permitieran la creación de un modelo base.

Así pues, Robert Kahn y Vint Cerf desarrollaron una variada arquitectura de interconexión de redes, basada en un determinado protocolo, que después de varios perfeccionamientos se convirtió en el Protocolo de Control de Transmisión - Transfer Control Protocol (TCP) o el Protocolo de Internet - Internet Protocol (IP).

Figura 3: El TCP/IP fue propuesto como el protocolo de comunicación estándar en ARPANET (1973).
Fuente: Freepik (2020), adaptado por labSEAD-UFSC (2020).

En 1973, el TCP/IP fue propuesto como el protocolo de comunicación estándar en ARPANET. Ese mismo año, se construyeron las primeras versiones de este protocolo que permiten la conectividad de extremo a extremo. A finales de los años 1970, varias redes locales y estaciones de trabajo experimentales, creadas por la comunidad de investigadores, se conectaron a la red ARPANET.

Las velocidades de transmisión de estas conexiones pioneras eran bajas comparadas con las actuales. Las transmisiones tenían respectivamente:

- 60Kbit/s para la red terrestre ARPANET.
- 400/100Kbit/s para la red de radio PRNET.
- 64Kbit/s para la red de satélites SATNET.

En este período de la historia no había computadoras personales, estaciones de trabajo o redes locales.

> Los dispositivos informáticos implicados en las conexiones eran las potentes máquinas de computación científica, que funcionaban en el sistema de compartir el tiempo y el trabajo entre los usuarios.

Los principales problemas en la construcción de la red inicial ARPANET estaban relacionados con la configuración de los ***gateways***, transformados más tarde en routers, para permitir la conexión de diferentes tipos de redes, así como el desarrollo de *software* en el estándar TCP/IP en las computadoras.

Un gateway, o puerta de enlace, es una máquina intermediaria destinada generalmente a interconectar redes, separar dominios de colisión o incluso traducir protocolos.

DÉCADA DE 1980

A principios de la década de 1980, se produjo una proliferación comercial de estaciones de trabajo personales y su conectividad a redes locales compatibles con Internet, lo que facilitó enormemente la interconexión de dispositivos a escala

exponencial. ARPA ya conectaba más de 500 centros, forzando la separación de la parte comercial de la red militar (MILNET).

Figura 4: El año de la aparición de internet. **Fuente:** labSEAD-UFSC (2020).

A finales de la década de 1980, Internet se hizo accesible también para uso comercial. Esto se estableció, principalmente, a través del servicio de *e-mail* autorizado para utilizar el *backbone* (columna vertebral de la red de Internet) para la comunicación con los usuarios con permiso de acceso a la red y las entidades federales de investigación interconectadas.

DÉCADA DE 1990

En esa década, la velocidad de transmisión de la información aumentó continuamente. Observa la diferencia en la velocidad de transmisión de una década a otra

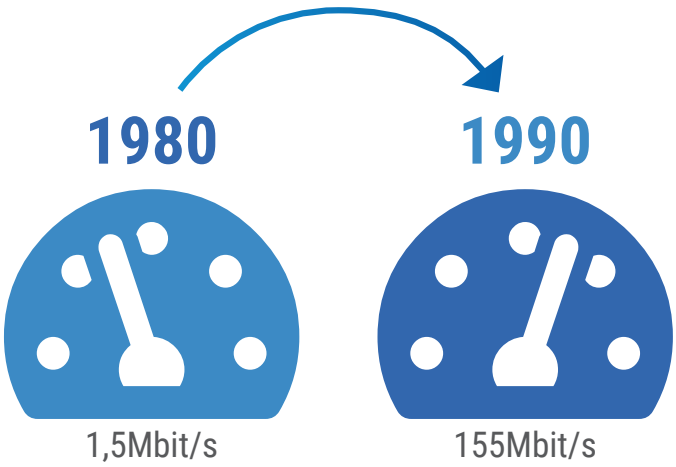


Figura 5: Diferencia de velocidad de la década de 1980 a 1990. **Fuente:** labSEAD-UFSC (2020).

Cabe señalar que en el momento de la ruptura con la red militar la ARPANET se trasladó definitivamente a lo que hoy se conoce como IPv4. La red siguió evolucionando hasta el punto de generar el agotamiento de este tipo de dirección "IP" en los decenios siguientes e impulsar la transición a IPv6. Profundizaremos en estos aspectos con más detalle más adelante.

Hasta finales de los años 1990, el control del acceso a Internet fue llevado a cabo por el Departamento de Defensa de los EE.UU., que fue testigo de la rápida expansión de su red a diferentes centros de investigación y de sus limitaciones para gestionar algo tan grande. ARPANET se extinguió y las organizaciones comenzaron a conectarse a otra red creada por la National Science Foundation Network (NSFNET), una organización no militar.

Después de 1990, el crecimiento de Internet fue simplemente espectacular, con aproximadamente un 10% mensual, debido a la inclusión de componentes comerciales e internacionales. Podemos citar tres momentos importantes.

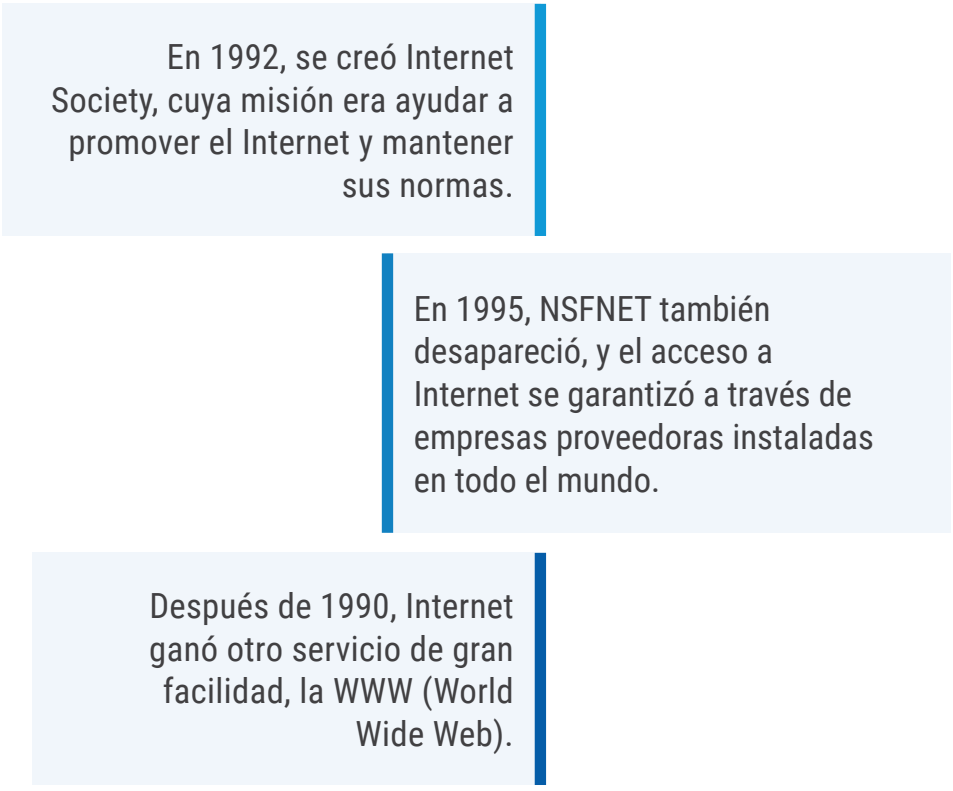


Figura 6: Momentos importantes para el crecimiento de Internet. **Fuente:** labSEAD-UFSC (2020).

Continúa tus estudios para comprender el concepto de Internet como una red compuesta por millones de computadoras en todo el mundo, que se comunican mediante el intercambio de datos.

Clase 2 – Concepto de Internet

CONTEXTUALIZANDO...

¿Has oído alguna vez la expresión “Internet de las cosas”? La rápida expansión de la red en los últimos años demuestra la magnitud del Internet en todo el mundo, aunque todavía haya poblaciones ubicadas en lugares salvajes que tienen poca o ninguna conectividad.

En este contexto, es importante comprender que Internet es un proceso en continuo crecimiento y que en sí misma representa un hito en el desarrollo de las tecnologías y, especialmente, de las comunicaciones.

EL FENÓMENO DE INTERNET

La creación de la computadora en la primera mitad del siglo pasado ya ha tenido un impacto significativo en la vida de las personas, revolucionando la industria y varios sectores de la producción de conocimientos.

El crecimiento de esta red de información es exponencial, transformando la forma de vida en el planeta a través de la migración de los hábitos y rutinas humanas al mundo digital. Dada la posibilidad de intercambiar información en tiempo real, en redes cada vez más rápidas, las actividades bancarias, las conversaciones, las prácticas comerciales, las instituciones educativas, entre otras actividades, han migrado a plataformas virtuales accesibles a través de Internet.

La conectividad entre países, personas y empresas a través de las redes informáticas, especialmente el Internet, es un fenómeno que distingue la etapa actual de desarrollo de la sociedad mundial.

> Entre los principales factores que hay que destacar en este reciente proceso evolutivo de la sociedad están: la invención de los dispositivos informáticos portátiles y la creación de la red informática mundial, llamada red Internet.

La vida en este ambiente artificial ha pasado de ser una mera invitación a lo necesario a vivir en la sociedad actual. Por ejemplo, el número de usuarios de las redes sociales supera la población de varios países: en 2016, la red social Facebook tenía 1,59 mil millones de usuarios, mientras que la población de China ascendía a 1,367 mil millones de ciudadanos, en el mismo período.

En la figura a continuación se pueden visualizar mejor los datos de la encuesta de usuarios y de la población mundial.

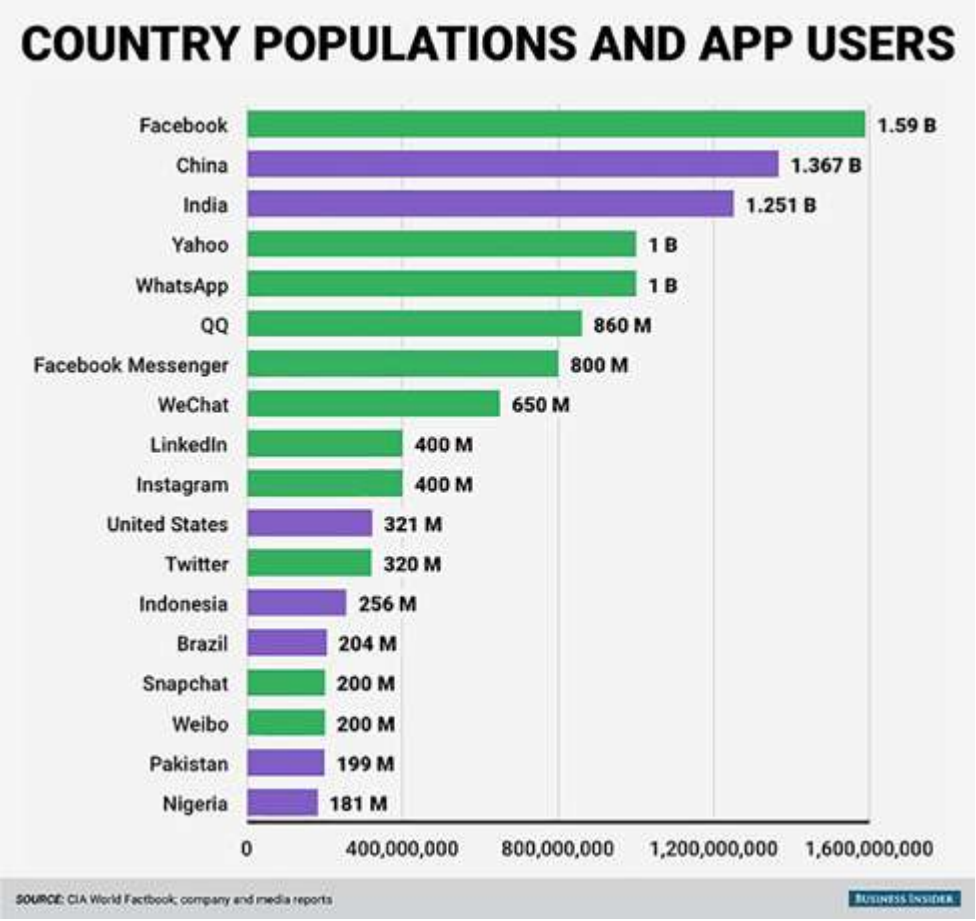


Figura 7: Relación de usuarios y población mundial. **Fuente:** Business Insider (2016).

Este fenómeno se extiende por todos los aspectos de las relaciones sociales. En lo que respecta a la economía mundial, las rápidas operaciones en programas y sistemas operativos, instalados en estos terminales de acceso, garantizan al usuario la resolución de problemas cotidianos que le costarían largos desplazamientos geográficos o el uso de herramientas manuales de gran coste físico o monetario.

> La aparición de aplicaciones de *e-commerce* y el crecimiento del mercado publicitario han redefinido antiguas formas de acción empresarial, que han ganado en dinamismo y rentabilidad, ya que los obstáculos físicos fueron superados por las facilidades aportadas por la tecnología de la información.

El siguiente ejemplo ilustra el impacto de la tecnología en las operaciones bancarias y demuestra cómo la conectividad informática cambia la forma de vida de la sociedad.

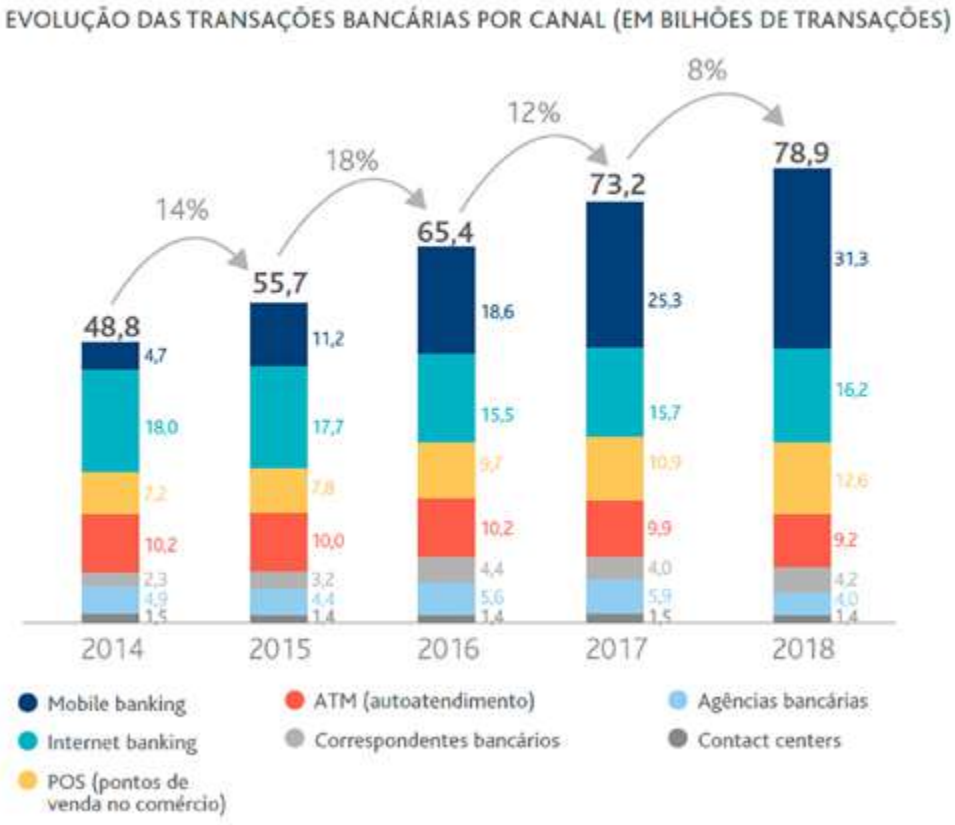


Figura 8: Aumento del número de transacciones bancarias por *Internet banking*.
Fuente: FEBRABAN (2019).

Nótese que en el 2014 el *mobile banking* representaba el 4,7% del total de las transacciones bancarias, mientras que en el 2018 este porcentaje se convirtió en el 31,3%. En este aspecto, el desarrollo de aplicaciones en entornos totalmente virtuales aportó innumerables beneficios a la vida humana. Podemos destacar algunos ejemplos:

- La expansión del acceso a la información en su conjunto.
- La democratización de la educación con plataformas de aprendizaje a distancia.
- Los sistemas de acreditación en general (matrícula escolar, registro de eventos, entre otros).
- Acceso a servicios de interés público (compra de billetes de avión, pago de facturas telefónicas, entre otros).

Universidades de todo el mundo han dedicado inversiones en investigaciones basadas en la tecnología informática, lo que ha dado lugar a novedades en las áreas de la salud, la comunicación, la ingeniería, las artes, la aritmética, etc.

Por consiguiente, la multiplicación de dispositivos capaces de acceder a los más diversos sitios de Internet ha permitido concentrar artefactos y herramientas vitales para el hombre moderno en un solo dispositivo, que puede ser una computadora de escritorio o un simple celular.

Figura 9: Dispositivos presentes en la vida moderna. **Fuente:** Pixabay (2020).

Debido a este fenómeno creciente y a la preocupación del Estado por consolidar una estructura de confrontación, este curso presenta una visión general de un nuevo tipo de criminalidad, el de naturaleza cibernética, presentando desde su génesis hasta los formatos más actuales y sofisticados, así como el conjunto técnico-procesal necesario para el desempeño profesional en estos casos.

INTERNET, COMPUTADORAS E INTERCONECTIVIDAD

El término Internet proviene de la combinación de las palabras inglesas *interconnect* y *network*. En 1883, se utilizó el término "internet", con una inicial en minúscula, como verbo y adjetivo para referirse a los movimientos interconectados.

> A principios de la década de 1970, el término *internet* comenzó a utilizarse como forma abreviada del conjunto de redes informáticas interconectadas mediante puertas de enlace o *gateways* especiales.

Por lo tanto, los términos *internet* e Internet tienen conceptos diferentes, compruébalo.

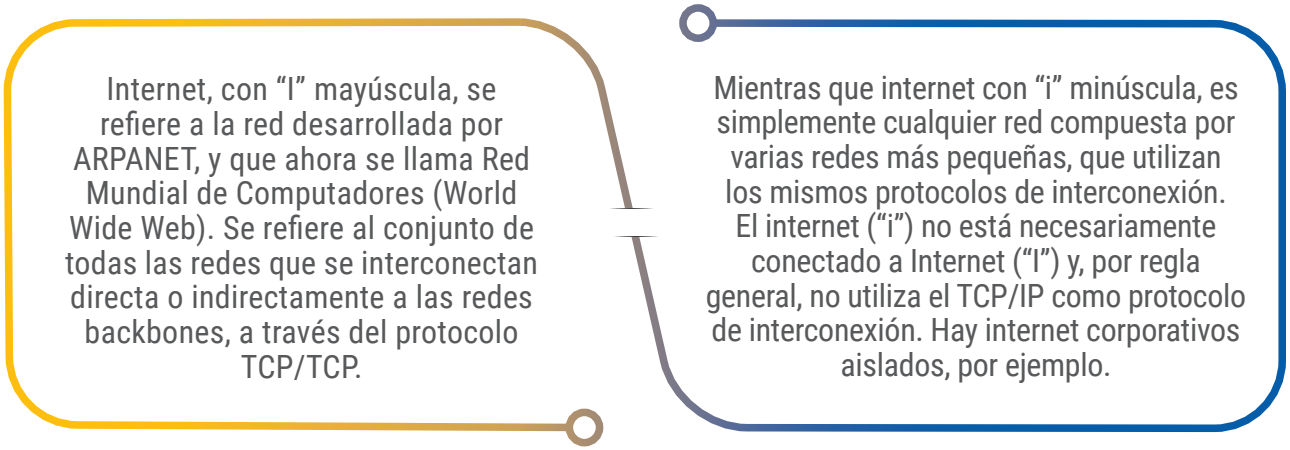


Figura 10: Diferencia entre los términos "internet" e "Internet". **Fuente:** labSEAD-UFSC (2020).

Es didácticamente interesante la comprensión de lo que es una red, expresión citada en los párrafos anteriores.

En el contexto de nuestros estudios, entenderemos la red como la situación en la que dos o más computadoras están interconectadas.

Las principales razones para tener una red son:

- Permitir que los usuarios de computadoras se comuniquen entre sí.
- Permitir el acceso remoto a los servicios ofrecidos por una computadora en red.

Las computadoras en Internet se conectan con la ayuda de cables de telecomunicación o inalámbricos, con la ayuda de antenas de satélite y líneas celulares.

> El término "computadora" utilizado en las líneas anteriores debe entenderse como un género, teniendo en cuenta la accesibilidad y la conectividad de la mayoría de los dispositivos electrónicos que se fabrican hoy en día.

Internet no solo se compone de computadoras domésticas o corporativas, sino también de teléfonos móviles, televisores y muchos otros dispositivos que se añaden diariamente a la red.

El Internet de las cosas

¿Has oído hablar de la expresión "Internet de las cosas" o "IoT" (Internet of Things)?

Se refiere a la extensión del poder de Internet, desde el uso de computadoras y *smartphones* hasta una variedad de otras cosas, procesos y entornos.

Figura 11: Conexión entre todas las cosas del mundo. **Fuente:** labSEAD-UFSC (2020).

La interconexión de estos dispositivos aporta ventajas prácticamente en todos los ámbitos, ya que los sensores de a bordo recogen información en todo momento de su entorno y alimentan depósitos de información capaces de fomentar una inteligencia analítica que responda al usuario.

Estos beneficios se obtienen con el uso de *smartphones, laptops* y *tablets*, por ejemplo. La popularidad de Internet se debe, principalmente, a la enorme posibilidad de intercambio y comunicación de información, así como a la facilidad de uso de sus servicios. De hecho, se admite que cualquier computadora puede conectarse a Internet fácil y rápidamente con un mínimo de equipo adicional.

Clase 3 - Nociones sobre el Funcionamiento de Internet

CONTEXTUALIZANDO...

¿Vamos a entender cómo funciona *internet*? En esta clase, presentaremos el Internet a través de la metáfora de la "red de comunicación". Para ello, comprenderás la diferencia entre la comunicación establecida por una línea telefónica, por ejemplo, y la establecida por paquetes, que permite el uso de la red por varios usuarios al mismo tiempo, lo que permite una comunicación rápida y eficaz.

¿CÓMO FUNCIONA INTERNET?

Dando continuidad a los contenidos vistos anteriormente, entenderemos el Internet como una gran red comunicacional formada por dispositivos informáticos conectados a redes autónomas interconectadas.

En general, estas conexiones operan de diferentes maneras, que podemos conocer con la siguiente imagen.

Figura 12: Funcionamiento de las conexiones. **Fuente:** labSEAD-UFSC (2020).

Desde una perspectiva funcional, Internet hace un trabajo muy simple: mueve informaciones computarizadas (datos) de un lugar a otro a través de sus dispositivos que conforman la red. Para ello, **todos los puntos de Internet tratan la información que manejan exactamente de la misma manera**.

Así pues, es comprensible que Internet funcione de manera similar a un servicio postal: las cartas y los paquetes simplemente se pasan de un lugar a otro, sin importar quién es el remitente y el destinatario, ni el contenido que se va a entregar.

En resumen, el trabajo del servicio postal es trasladar las cartas de un lugar a otro, sin importar por qué la gente escribe cartas, tal como sucede en Internet.

> Esta objetividad simplificada con respecto al flujo de Internet también ha demostrado la capacidad de la red para manejar la amplia variedad de información, permitiendo a los usuarios realizar diversos trabajos y de distinta naturaleza.

Toda la información se trata de igual manera y se transmite exactamente de la misma manera. Así que, a través de internet, podemos:

- Realizar tareas como el envío y la recepción de *e-mails*.
- Mostrar páginas *web*.
- Mensajes de chat.
- Procesar los comandos en los dispositivos de IoT.

Con la posibilidad de tratar y transmitir la información de la misma manera, se estimuló el desarrollo de nuevas aplicaciones, es decir, nuevas soluciones tecnológicas, que se ejecutan en la parte superior de la red básica de computadoras y dispositivos informáticos en general.

Saber más

Janus Friis y Niklas Zennstrom fueron los inventores europeos que desarrollaron Skype, una herramienta para hacer llamadas telefónicas por Internet. Necesitaban escribir un programa que pudiera transformar el habla en datos de Internet y así establecer una conversación virtual.

Como hemos visto antes, gran parte de Internet funciona en la red telefónica pública ordinaria, pero hay una gran diferencia entre el funcionamiento de **una llamada y la forma en que Internet transporta los datos.**

Red telefónica: conmutación de circuitos

La conmutación de circuitos puede ser vista como una forma realmente ineficiente de usar una red. Una llamada a través de un teléfono fijo, por ejemplo, siempre abre una conexión directa (o un circuito) entre un punto, que puede ser una residencia, y otro terminal. Durante todo el tiempo que esté conectado a otra residencia, nadie más puede contactarlo por teléfono. Supongamos que un usuario habla demasiado despacio por teléfono, deja largos espacios de silencio o deja su auricular "descolgado" durante la llamada, este circuito permanecerá permanentemente abierto entre sus dos teléfonos.

Esta forma de conectar los teléfonos se llama conmutación de circuitos. Incluso si no estás enviando información en línea, el circuito sigue conectado y por lo tanto impide que otras personas lo usen.

Saber más

A mediados del siglo pasado, cuando se hacía una llamada, alguien tenía que meter y sacar los cables de una "centralita telefónica" (literalmente, un tablero de madera con cables y enchufes por todas partes) para crear circuitos temporales que conectaban una casa con otra. Hoy en día este circuito se conmuta automáticamente mediante una central telefónica electrónica.

Ahora que conocemos la conmutación de circuitos, seguimos para conocer la conmutación de paquetes.

Internet: conmutación de paquetes

En teoría, Internet podría funcionar mediante la conmutación de circuitos. Las primeras conexiones a la red fueron por marcación ***dial-up***, cuando la computadora marcó un número de teléfono para ponerse en contacto con el proveedor de servicios de Internet en una llamada telefónica normal.

Dial-up es una forma de acceso a la internet que utiliza la red telefónica pública conmutada para establecer una conexión de acceso a internet a través de un número de teléfono a una línea telefónica.

En este caso, la conmutación de circuitos se usó para entrar *on-line*.

¿La marcación por Internet todavía existe?

Esto era un gran inconveniente, porque nadie podía llamar mientras estaba en línea, y los cargos por los servicios de los operadores se hacían por cada segundo que permanecía en la red. Finalmente, la conexión a Internet se estableció muy lentamente.

Figura 13: La famosa Internet *dial-up*.
Fuente: labSEAD-UFSC (2020).

Actualmente, los datos se mueven por Internet de una manera completamente diferente, llamada conmutación de paquetes.

En la Práctica

Imaginen un pedido de envío de un *e-mail* a alguien en otro país: en lugar de abrir un circuito largo y complicado entre la casa del remitente del *e-mail* y el país de destino del mensaje, el *e-mail* se divide en pequeñas piezas llamadas paquetes. Cada uno está marcado con su destino final y puede viajar por separado. Teóricamente, todos los paquetes podrían viajar por rutas totalmente diferentes. Cuando llegan a su destino final, son reensamblados para enviar un *e-mail* de nuevo.

La conmutación de paquetes es mucho más eficiente que la conmutación de circuitos. No es necesario tener una conexión permanente entre los dos lugares de comunicación, lo que evita bloquear toda una parte de la red cada vez que se envía un mensaje. Por lo tanto, muchas personas pueden utilizar la red al mismo tiempo, facilitando una comunicación más rápida y eficiente.

Debido a que los paquetes pueden fluir a través de muchas rutas diferentes, dependiendo de cuál es más silenciosa o más ocupada, toda la red se utiliza de manera más uniforme.

Curiosidad

Figura 14: Paul Baran.
Fuente: Wikipedia (2020).

Paul Baran, considerado uno de los pioneros de Internet, perfeccionó las técnicas de conmutación de paquetes y las aplicó al proyecto que daría lugar a la red ARPANET. Su trabajo desempeñó un papel clave en el desarrollo de Internet.

En la década de 1960, Paul Baran se unió a una entidad que desarrollaba investigación y análisis para el Departamento de Defensa de los Estados Unidos, llamada RAND,

acrónimo de Research and Development Corporation, donde trabajó en el desarrollo de un sistema de comunicaciones que pudiera sobrevivir al daño de un arma nuclear.

Según RAND, una de las mayores preocupaciones era que ni la central telefónica de larga distancia ni la red de mando y control militar sobrevivirían a tal ataque. Aunque la mayoría de los *links* no estaban dañados, las instalaciones de conmutación centralizadas serían destruidas por los enemigos.

En consecuencia, Baran diseñó un sistema que no tenía conmutadores centralizados y que tenía la capacidad de funcionar incluso si muchos de sus *links* y nodos de conmutación eran destruidos. Originalmente, llamó al proceso "bloqueos de mensajes". Otros científicos, entre ellos Donald Davies, que más tarde cambiaría el nombre por el de "conmutación de paquetes", también llegaron a una conclusión similar al mismo tiempo.

Este concepto de conmutación de paquetes, que consiste en un método de comunicación digital que implica el movimiento de datos, divididos en lo que Baran llamó **"bloques de mensajes"** en redes compartidas y distribuidas, fue la esencia tecnológica de ARPANET, que más tarde evolucionaría hacia Internet.

Baran imaginó una red de nodos no tripulados que actuaría como conmutadores, enviando la información de un nodo a otro hasta sus destinos finales. Los nodos utilizarían un esquema que Baran llamó **"comunicaciones distribuidas"**.

Eso nos lleva al final de otra clase. ¡Sigamos para obtener más conocimiento!

Clase 4 – Principales Protocolos de Internet

CONTEXTUALIZANDO...

Internet realiza la sencilla tarea de trasladar información computarizada de un lugar a otro a través de sus dispositivos de red. En esta clase, comprenderemos cómo funcionan las transmisiones de datos, los principales protocolos de comunicación y cómo es posible realizar ciertos comandos a través de esta tecnología.

¡Continúa tus estudios y compruébalos!

TRANSMISIÓN DE DATOS

Esta transmisión de datos se produce con la máxima fluidez entre todos los puntos de Internet, porque son capaces de interpretar infaliblemente lo que les llega. Esto solo es posible debido a la existencia de protocolos comunes a todos. De esta manera, pueden tratar la información que manejan exactamente de la misma manera.

En realidad, lo que ocurre, técnicamente, cuando se hace el comando “enviar” en un mensaje de *e-mail*, es que se abstrae del usuario, pareciendo un proceso extremadamente simple.

El remitente no tiene la menor idea de que su “clic” impulsa la acción de varios protocolos y que se inicia una operación compleja de un sistema de información.

Figura 15: Protocolos de programación. **Fuente:** Pixabay (2020).

Estos protocolos constituyen un conjunto de normas que permiten que cualquier dispositivo conectado a Internet se comunique con otro también conectado a la red, como una especie de "lenguaje universal" entre las computadoras, independientemente del fabricante y del sistema operativo utilizado. Esto hace innecesario el uso de cualquier tipo de *software* extra para que una computadora pueda entender los protocolos de la red.

Protocolos de comunicación de Internet

La base de la comunicación de la red en Internet es la acción de unos 500 protocolos específicos. Esta colección de protocolos se llama **"Familia de Protocolos de Internet"** o **"Familia TCP/IP"**.

A continuación se indican los protocolos más importantes que se utilizan comúnmente en las comunicaciones a través de la red de Internet. Presentaremos los acrónimos junto con una traducción no oficial, para entender el propósito de cada uno, verifica el siguiente cuadro:

Protocolos Principales ↓	**Telnet** Protocolo de Acceso Remoto Telnet	**FTP** Protocolo de Transferencia de Archivos	**SNMP** Protocolo Simple de Gerenciamento de Red
IP Protocolo de Internet	**SSH** Protocolo de Acceso Remoto del Secure Shell	**XMPP** Protocolo Extensible de mensajes y presencia	**IGRP** Protocolo de Reenvío de Gateway Interior
DHCP Protocolo de Configuración Dinámica de Hosts	**POP3** Protocolo de Agencia Postal 3	**NDMP** Protocolo de gestión de Datos de Red	**EIGRP** Protocolo de Reenvío de Gateway Interno Mejorado
HTTP Protocolo de Transferencia de Hipertexto	**SMTP** Protocolo de Transferencia Simplificada de e-mai	**L2TP** Protocolo de encapsulación de capas 2	**BGP** Protocolo de Gateway de Frontera
HTTPS Protocolo de Transferência Segura de Hipertexto	**IMAP** Protocolo de Acceso a Mensajes de Internet	**NTP** Protocolo de Cobertura de Red	**PPP** Protocolo Punto a Punto
TCP Protocolo de Control de Transmisión	**NNTP** Protocolo de transferencia de Noticias en Red	**SCTP** Protocolo de Transmisión de Control de Flujo	**ARP** Protocolo de Resolución de Direcciones
UDP Protocolo de Datagrama de Usuario	**RIP** Protocolo de Informaciones de Reenvío	**TLS** Seguridad de Capas de Transporte	**RARP** Protocolo de Resolución de Dirección Inversa

Quadro 1: Lista de protocolos que forman el lenguaje universal de las computadoras. **Fuente:** labSEAD-UFSC (2020).

De esta manera, un terminal puede comunicarse con otro conectado a la red mundial. A medida que este "lenguaje" es interpretado por todas las máquinas por igual, la conectividad se vuelve universal y la gran red de información se expande cada día.

La siguiente pila de protocolos está dividida en 4 capas.

1

Aplicación: en esta capa actúan los protocolos utilizados por los programas para enviar y recibir datos a través de Internet. No hay una norma común, siendo esta establecida por cada solicitud. Es decir, FTP tiene su propio protocolo, así como TELNET, SMTP, POP3, HTTP, DNS, etc.

2

Transporte: capa responsable de transportar los archivos recibidos de la capa anterior. Aquí es donde se organiza y se transforma en paquetes más pequeños, que serán enviados a la red. Es una capa de extremo a extremo, es decir, una entidad de esta capa solo se comunica con su lado de entidad del anfitrión receptor. Es en esta capa donde se controla la conversación entre las aplicaciones intercomunicadas de la red. Aquí se utilizan dos protocolos: TCP y UDP. El TCP está orientado a la conexión y el UDP no. El acceso de las aplicaciones a la capa de transporte se realiza a través de puertos que reciben un número entero para cada tipo de aplicación.

3

Internet o Red: esta capa fue la primera estandarizada en el modelo. Se encarga de dirigir, encaminar, enviar y recibir el control. No está orientado a la conexión, se comunica a través de datagramas. Estos archivos empaquetados en la capa anterior se reciben y se adjuntan a la IP de la máquina que envía y recibe los datos. Desde aquí se envían a través de Internet usando la siguiente capa.

4

Interfaz o enlace: aquí es donde se ejecuta la recepción o el envío de archivos en la *web*, ya que también corresponde a la capa física. Es el espacio reservado para diversas técnicas de transmisión de datos de un punto a otro.

Figura 16: Los grupos que componen la subdivisión de los protocolos. **Fuente:** labSEAD-UFSC (2020).

El funcionamiento de la **red Internet** está directamente **vinculado** al más importante de todos los protocolos: **el TCP/IP**. Entre todos los protocolos existentes y funcionales de la red, el trabajo conjunto de estos dos protocolos forma la estructura para enviar y recibir datos a través de Internet.

La familia de protocolos de Internet sigue esta perspectiva y continúa evolucionando. Siempre se publican nuevos estudios en la red por parte de las universidades especializadas, así como las innovaciones aportadas por los mecanismos de solicitud de observaciones (RFC, en inglés *request for comments*).

Los nuevos protocolos (la mayoría de los protocolos de aplicación) que actualmente diseñan y aplican los investigadores y científicos están expuestos a la comunidad de Internet en forma de RFCs.

Dirección MAC y dirección IP

Como vimos en la clase anterior, el TCP/IP es el acrónimo de dos protocolos combinados: el TCP (Protocolo de Control de Transmisión, en inglés Transmission Control Protocol), y la IP (Protocolo de Internet, en inglés Internet Protocol).

Es común confundir el protocolo IP con la dirección MAC (Media Access Control), cuando se está direccionando.

> La principal diferencia entre ellos es que la dirección MAC se utiliza para garantizar la dirección física de la computadora, mientras que la IP se utiliza para identificar de manera exclusiva la conexión de la red.

En general, **la dirección MAC y la dirección IP se utilizan para definir un dispositivo en Internet**, pero mantienen sus propias peculiaridades: la dirección MAC individualiza un dispositivo y la IP individualiza un punto de conexión.

Verifícalo:

El fabricante de la tarjeta NIC proporciona la dirección MAC, donde cada dispositivo de red tiene una dirección MAC *address* de 12 caracteres, que siempre lo individualizará en el mundo de Internet.

La dirección MAC puede entenderse como si fuera una "tarjeta de identificación" o una "huella dactilar" de un dispositivo de red, ya que este "identificador" es permanente y único.

Observa el siguiente ejemplo de una dirección **MAC 50-BC-93-EF-5B-0C**.

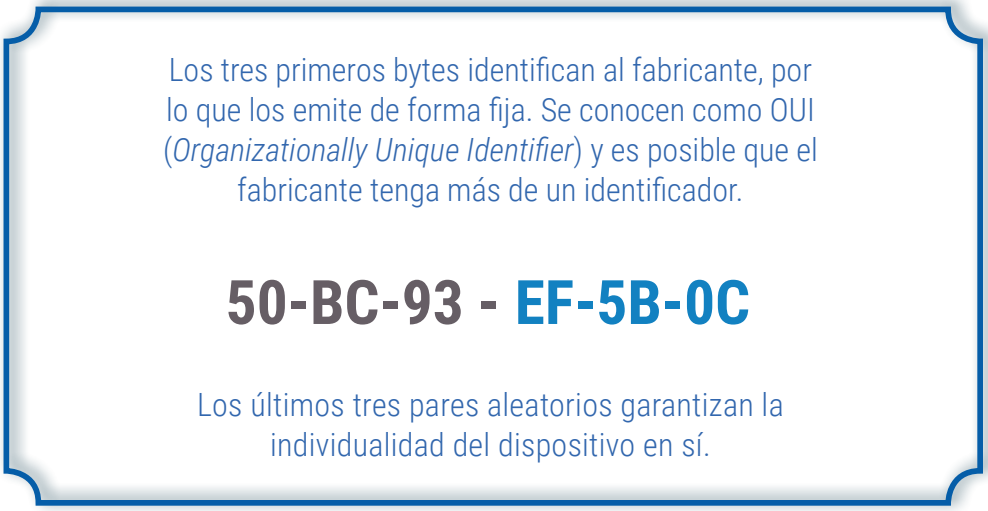


Figura 17: Funcionamiento de una dirección MAC. **Fuente:** labSEAD-UFSC (2020).

Debido a que es única y estática, la dirección MAC le permite identificar eficientemente los dispositivos en la red cuando no se conoce la dirección IP. Esta tecnología es efectiva para detectar la ubicación de un dispositivo específico. También puede utilizarse para conectar o restringir direcciones.

El proveedor de servicios de Internet proporciona la dirección IP, desde la que el dispositivo participa en una red. Se individualiza en esta red exclusivamente por su dirección física (MAC Address).

De manera diferente, pero complementaria, el direccionamiento IP permite la comunicación entre dispositivos a través de Internet, porque a partir de la identificación, los *softwares* clientes se conectan a esta dirección.

Clase 5 – El Protocolo IP: Tipos y Características

CONTEXTUALIZANDO...

¿Por qué se considera el protocolo IP como uno de los principales protocolos de Internet?

En esta clase comprenderemos por qué necesitamos direcciones IP, los tipos de direcciones que existen, las versiones y lo que cambia en la característica de una IP a otra.

EL PROTOCOLO IP

El protocolo IP se encarga de dirigir y fragmentar los paquetes de datos en las redes digitales. Junto con la capa de transporte el Protocolo de Control de Transmisión (TCP), forman la base de Internet.

Cuando se envía un paquete del remitente al destinatario, el protocolo IP crea una estructura de paquetes que resume las informaciones enviadas en **datagramas**. Así pues, determina la forma en que se describen los datos sobre el origen y el destino de los paquetes y los separa del resto escritos en el encabezado.

El datagrama de IP es la unidad básica de datos a nivel de IP. Un datagrama se divide en dos áreas, un área de encabezado que contiene toda la información necesaria que identifica el contenido del datagrama, y un área para otros datos en la que se encapsula el paquete de nivel superior, es decir, un paquete TCP o UDP.

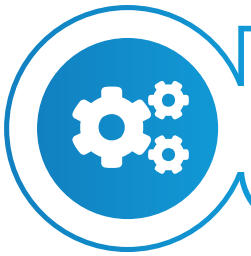
Actualmente se utilizan dos versiones del protocolo IP: **IPv4** e **IPv6**. El número de versión está relacionado con la versión del protocolo TCP utilizado.

Aunque no hay más publicaciones desde IPv4 e IPv6, el protocolo de Internet ha sido revisado desde su primera mención en 1974. La atención se centró esencialmente en la optimización de la configuración y el direccionamiento de la conexión. Por ejemplo, se aumentó la longitud de *bits* de las direcciones de *host* de 16 a 32 *bits*, ampliando este espacio a aproximadamente 4.000 millones de posibles *proxies*.

IPv4

Es la primera versión del protocolo de Internet que entró en vigor, publicada en 1984. Antes de eso, solo era parte del TCP y no existía de forma independiente.

En la versión más común, IPv4 consiste en una secuencia de números, separados por puntos. Por lo tanto, se presenta en el siguiente formato: **x. x. x. x**, donde x se denomina "octeto" (8 *bits*) y debe ser un valor decimal entre 0 y 255.



En la Práctica

Una dirección IPv4 está compuesta por cuatro octetos separados por tres puntos. Un ejemplo sería: 187.121.172,10.

Con el fin de crear un formato más expandible que ofrezca más opciones, el IPv6 fue definido en diciembre de 1998 por el IETF (Internet Engineering Task Force - Grupo de Tareas de Ingeniería de Internet). Según la publicación de una especificación estándar de Internet, RFC 2460, utilizaría 128 *bits*, en 16 octetos de 8 *bits*, presentados en forma hexadecimal de 0-9 + AF-.

IPv6

El IPv6 es el sucesor directo del IPv4, ya que el desarrollo de IPv5 se suspendió prematuramente por razones económicas.

Se considera que el IPv6 es una evolución en relación con el IPv4, ya que consta de campos de direcciones de 128 *bits*, que permiten unas 340 sextillones (un número con 37 ceros) de secuencias diferentes, satisfaciendo así la necesidad de direcciones de Internet a largo plazo.

La dirección IPv6 se constituye entonces en el siguiente formato: **y: y: y: y: y: y: y: y.** Llamamos a la Y segmento y puede ser cualquier valor hexadecimal entre 0 y FFFF.

Los segmentos están separados por dos puntos, no por un punto, observe los ejemplos:

- 2804: ec8: 3333: 4444: 5555: 6666: 7777: 8888.
- 2208: ec8: 3333: 4444: CC0: DDDD: EEEE: FFFF.

Una dirección IPv6 normal debe tener ocho segmentos como estándar, aunque se permite una especie de notación abreviada para los segmentos.

En la Práctica

Has podido observar que los segmentos son ceros o con ceros a la izquierda, en este caso, se permite una especie de abreviatura, comprueba a continuación algunos ejemplos de segmentos abreviados:

- IPv6 - 2804: ec8:: - los últimos seis segmentos son cero.
- IPv6 - :: 1234: 5678 - los primeros seis segmentos son cero.
- IPv6 - 2804: ec8:: 1234: 5678 - los cuatro segmentos centrales son cero.

También puedes comprimir el segmento para eliminar los ceros de la izquierda, como sigue:

IPv6 - 2804: 0ec8: 0001: 0000: 0000: 0ab9: C0A8: 0102.
IPv6 - 2804: ec8: 1 :: ab9: C0A8: 102 (versión comprimida).

El despliegue del IPv6 se justificaba por la limitación del número de direcciones IP en relación con el crecimiento exponencial del número de usuarios de Internet.

Con la llegada de los dispositivos de IoT (Internet de las Cosas) conectados a la red, esta demanda se incrementó a una velocidad aún mayor, lo que dio lugar a la necesidad de desplegar redes locales corporativas. Para proporcionar accesibilidad a todos los usuarios y satisfacer demandas específicas, las direcciones se subdividieron en clases.

La clase de dirección

Incluso antes de la llegada de los dispositivos de IoT, cuando las computadoras eran todavía las únicas en el mundo, hubo una gran proliferación de máquinas en el ambiente de los negocios en todo el mundo.

El flujo operativo de la gran mayoría incluía definitivamente la informática en los procesos internos de estas organizaciones.

> Para el despliegue de las redes locales a nivel empresarial, así como para el acceso a la red de Internet por parte de nuevos usuarios, se necesitaban direcciones IP disponibles.

A continuación se elaboró un plan de distribución establecido por la Autoridad de Asignación de Números de Internet (IANA) y la Corporación de Asignación de Nombres y Números de Internet (ICANN), que básicamente dividió las direcciones en tres clases principales y dos clases complementarias.

Se dividen en: **clase A, clase B, clase C, clase D** y **clase E**. ¡Observa los detalles de cada tipo de dirección abajo!

Clase A

Permite hasta 128 redes, cada una con hasta 16.777.214 dispositivos conectados.

Ejemplo: 0.0.0.0 hasta 127.255.255.255.

Las direcciones IP de clase A se utilizan en lugares donde se necesitan pocas direcciones de red, pero donde hay un gran número de dispositivos conectados a ellas. Para ello, el primer *byte* se utiliza como identificador de la red y los demás sirven como identificadores de los dispositivos conectados (*notebooks*, *smartphones*, impresoras, etc.).

Clase B

Permite hasta 16.384 redes, cada una con hasta 65.536 dispositivos.

Ejemplo: 128.0.0.0 hasta 191.255.255.255.

Las IP de la clase B se utilizan en los casos en que existe cierta equivalencia en cuanto al número de redes y el número de dispositivos. Los dos primeros *bytes* de la dirección IP se utilizan para identificar la red y el resto para identificar los dispositivos.

Clase C

Permite hasta 2.097.152 redes, cada una con hasta 254 dispositivos.

Ejemplo: 192.0.0.0 hasta 223.255.255.255.

La clase C es adecuada para lugares que requieren un gran número de redes, pero con pocos dispositivos asignados a cada una. Así, los tres primeros *bytes* se utilizan para identificar la red y el último se utiliza para identificar las máquinas.

Classes D y E

La **clase D** es llamada ***multicast***, y las direcciones de la **clase E** son ***multicast* reservadas**.

Ejemplo clase D: 224.0.0.0 hasta 239.255.255.255.
Ejemplo clase E: 240.0.0.0 hasta 255.255.255.255.

Las clases D y E existen por razones especiales: la primera se utiliza para la propagación de paquetes especiales para la comunicación entre dispositivos, mientras que la segunda se reserva para aplicaciones futuras o experimentales.

¿Sabía que además de estas direcciones, tenemos varios bloques de direcciones reservados para fines especiales?

Observa más detalles a continuación.

Direcciones reservadas

Una dirección que comienza con 127 suele indicar una **red "falsa"**, es decir, que se utiliza solo para hacer pruebas. En el caso de la dirección 127.0.0.1, por ejemplo, suele referirse al propio dispositivo, es decir, al **propio *host***, lo que hace que se llame ***localhost***.

La dirección 255.255.255.255 se utiliza para **propagar mensajes** a todos los *hosts* de una red simultáneamente.

> También son dignos de mención los conjuntos de direcciones de las **clases A**, **B** y **C**, que son **"privadas"**. Esto significa que no pueden utilizarse en Internet, ya que se reservan para aplicaciones locales.foram reservados para aplicações locais.

Las **direcciones IP privadas**, como ya se explica en su propia terminología, están destinadas a ser utilizadas en redes privadas como las redes domésticas y de oficina. Son esencialmente estos:

- Clase A: 10.0.0 a 10.255.255.255.
- Clase B: 172.16.0.0 a 172.31.255.255.
- Clase C: 192.168.0.0 a 192.168.255.255.

Las **IP privadas** tienen la misma constitución que las direcciones IP públicas, sin embargo, solo pueden utilizarse dentro de una red interna porque su direccionamiento no es comprensible para otras redes autónomas. Del mismo modo, una computadora solo es accesible dentro de una red local cuando está conectada a una dirección IP privada que le ha dado la administración.

En este caso, como cada dispositivo de la red tendría solo una dirección IP privada, solo podría ser visto por otros dispositivos de la misma red local. Teóricamente, no estarían dirigidas a su uso en la Internet en general.

LAN es la Red de Área Local. Se conocen como Redes de Área Local, o Redes Locales, que conectan las computadoras presentes en el mismo espacio físico.

En caso de que uno de los dispositivos de red **LAN** quiera ser accesible a la red de Internet, entonces, debe conectarse a través de una dirección **IP pública**.

Las direcciones IP públicas son las otras direcciones IP que no incluyen ninguna de las direcciones IP privadas reservadas por los grupos estándar de Internet.

> Lo que le permite a una computadora perteneciente a una red local conectarse simultáneamente a la Internet es la tecnología incorporada en los routers o las unidades de combinación de **módem** y **router**.

Estos artefactos electrónicos sirven esencialmente como un puente entre una red privada e Internet.

Estos son los pasos para el funcionamiento del módem/router.

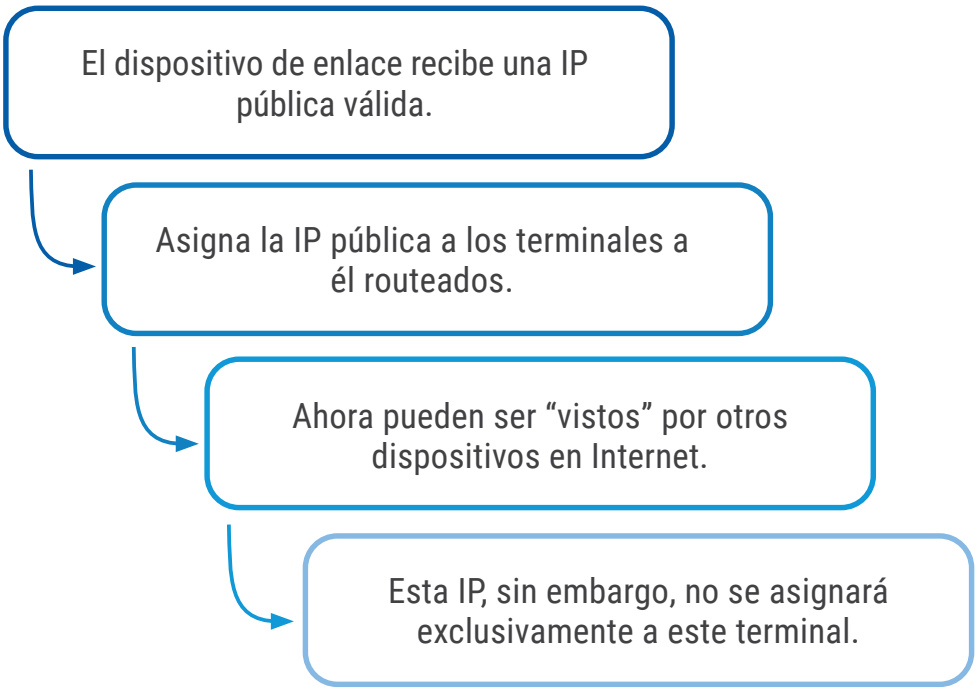


Figura 18: Cómo funciona la conexión de la red local. **Fuente:** labSEAD-UFSC (2020).

Desde una perspectiva externa, todos los dispositivos de la red doméstica se comunican con Internet desde una única dirección IP pública.

Figura 19: Las entradas del router son las LANs. **Fuente:** Pixabay (2020), adaptado por labSEAD-UFSC (2020).

Podemos entender esto: una red doméstica típica, un router tienen una dirección IP pública en Internet, y las computadoras, *smartphones,* las consolas de juegos y otros dispositivos conectados a ella tienen una dirección IP privada exclusiva de esa red local.

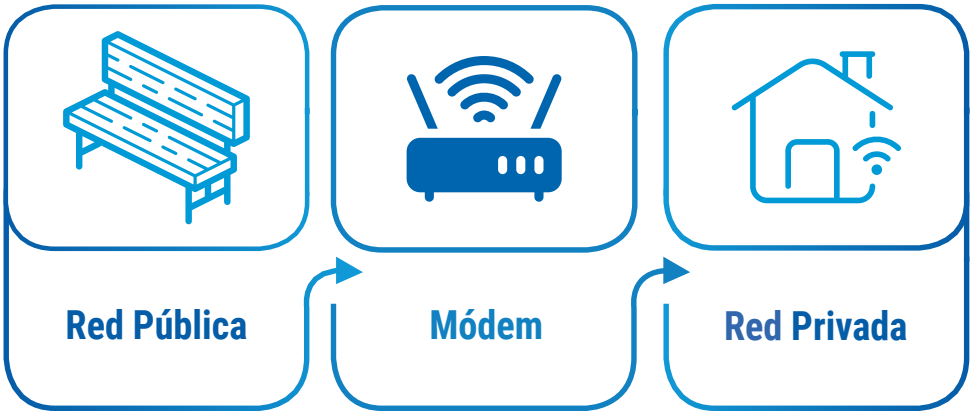


Figura 20: El router desempeña el papel de una IP pública. **Fuente:** labSEAD-UFSC (2020).

Cuando hablamos de grandes corporaciones, cada computadora tiene que tener una dirección IP distinta. Para ello, se utilizan recursos de asignación de direcciones IP más inteligentes. Uno de ellos es el protocolo **DHCP** (Dynamic Host Configuration Protocol).

> La característica importante de la DHCO es que permite a las computadoras obtener una dirección IP automáticamente de la red. La idea es automatizar esta configuración de las direcciones de las máquinas.

La ventaja de desplegar un servidor DHCP es que hace que las máquinas de direccionamiento sean más dinámicas que estáticas. Suele ocurrir de la siguiente manera.

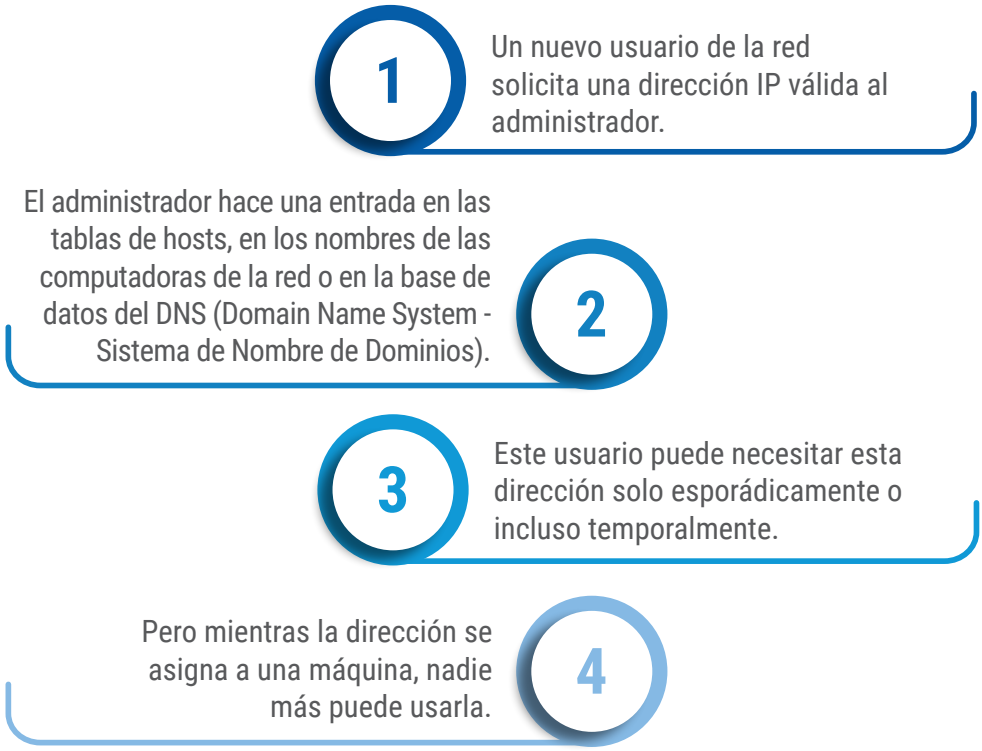


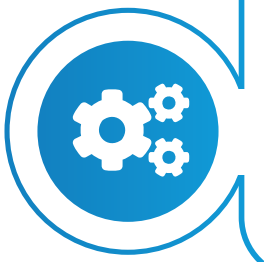
Figura 21: El DHCP es la mejor alternativa a través de las IP dinámicas. **Fuente:** labSEAD-UFSC (2020).

Dentro de los entornos corporativos, sus redes locales utilizan IPs dinámicas, proporcionando un amplio rango de direcciones IP privadas para sus máquinas. Como no hay una IP fija, cuando una computadora “entra” en la red, se le asigna una nueva IP que no está siendo utilizada por ningún otro terminal.

Puede ocurrir que se trate de una dirección que una vez se le asignó por un cierto período de tiempo a un usuario, pero que se libera porque ya no está en la red. Esto se debe a que en el

direccionamiento dinámico, teóricamente, en cada sesión el sistema de enrutamiento distribuirá una IP a cada dispositivo.

En la Práctica



En una empresa, los usuarios utilizan dispositivos móviles y se trasladan de una red del edificio a otra, y la dirección antigua puede funcionar en la nueva red local. Te das cuenta de que solicitar una dirección al administrador de la red local, solo para uso temporal, es un verdadero desperdicio. ¿Qué hacer?

El DHCP elimina este problema por medio de un proceso simple: asigna automáticamente las direcciones según se requiera y luego las libera cuando ya no se necesitan.

Cuando el sistema de un cliente de la red se inicia, envía automáticamente un mensaje solicitando una dirección. Debido a que un servidor DHCP tiene un grupo de IPs válidas asignables a los clientes y responde con una dirección generada dinámicamente.

> El protocolo DHCP es el método más utilizado para la distribución de IPs dinámicas. La **IP dinámica** es el número que se le dá a un dispositivo cuando se conecta a la red, pero que puede cambiar cada vez que haya una nueva conexión.

Las **IPs dinámicas** son más adecuadas para las empresas que para los hogares. Son esenciales para los servicios dedicados como el correo, el FTP y servidores *web*. La eficiencia del DHCP es su gran alojamiento de servidores informáticos, porque facilita la geolocalización de *hosts*. Piensa en el costo con rutinas de reconfiguración constante con el cambio de IP en un direccionamiento dinámico.

Los proveedores de servicios de Internet también trabajan con dinamismo en la asignación de direcciones. Cada vez que se solicita una conexión a Internet desde un punto de acceso en el que se encuentra un usuario, el proveedor proporciona una IP pública gestionada por él que es gratuita. Por razones de economía y disponibilidad, los proveedores de servicios de Internet adoptan esta tecnología.

La **IP estática**, a su vez, es una **dirección inalterable**. Así, el dispositivo mantendrá la misma IP mientras esté conectado a la red, incluso si renueva su asignación de direcciones. Este tipo de dirección es más adecuada para los individuos, porque tiene una fácil geolocalización.

Clase 6 – Protocolos HTTP y HTTPS: Internet y la *Web*

CONTEXTUALIZANDO...

Entre la lista de protocolos presentados anteriormente, destacamos los siguientes:

- IP - Protocolo de Internet.
- DHCP - Protocolo de Configuración Dinámica de Hosts.
- HTTP - Protocolo de Transferencia de Hipertexto.
- HTTPS - Protocolo de Transferencia Segura de Hipertexto.
- TCP - Protocolo de Control de Transmisión.

Hasta ahora, hemos centrado nuestros estudios en los tres primeros protocolos, para entender cómo funcionan las direcciones en la red y el tráfico de paquetes de datos.

En esta clase, hablaremos del protocolo de transferencia de hipertexto, **o HTTP**, y veremos cómo se ejecuta su principal función: **permitir la recuperación de los recursos enlazados por la *web***.

HTTP HTML

El protocolo HTTP fue desarrollado junto con el lenguaje HTML para crear el primer navegador interactivo basado en texto: la World Wide Web original. Hoy en día, el protocolo sigue siendo uno de los principales medios de uso de Internet. Para entender cómo funciona el protocolo HTTP, primero debemos entender la historia del lenguaje HTML.

HTML

El HTML (Hypertext Markup Language) fue creado en 1945 por el CERN (Organización Europea de Investigaciones Nucleares) con el fin de desarrollar, con fines militares, un sistema basado en enlaces entre recursos de información.

En 1965, el investigador Ted Nelson creó el término ***hyperlink***, al desarrollar un sistema de hipertexto a través del cual era posible compartir una variedad de información utilizando Internet, que en ese momento se utilizaba para la comunicación entre los investigadores nucleares que formaban parte del CERN.

Veamos la trayectoria de Tim Berners-Lee en la siguiente imagen.

1989

Para muchos, esta estructura conectada electrónicamente sería una especie de "embrión" que más tarde permitiría a Tim Berners-Lee escribir la primera propuesta para la World Wide Web. Aún en la década de 1980, el visionario Tim ya vio los problemas que hoy se llaman **accesibilidad digital**.

1990

En mayo de 1990, Berners-Lee escribió una segunda propuesta, con el apoyo del ingeniero de sistemas belga Robert Cailliau para la formulación de su propuesta. Este documento esbozó los principales conceptos y definió los términos importantes que hay detrás de la *web*. Su contenido describe un "proyecto de hipertexto" llamado World Wide Web, en el que una ***web* de documentos de hipertexto podía ser vista por los navegadores**.

Ya en el decenio de 1990, millones de computadoras se estaban conectando a través de la Internet, que se estaba desarrollando rápidamente, y se dio cuenta de que podían compartir información explorando una tecnología emergente llamada "hipertexto".

1991

Sin embargo, no fue hasta 1991 que el estadounidense Tim Berners-Lee publicó oficialmente un documento con una descripción del lenguaje HTML.

1994

En 1994, Tim se trasladó del CERN al Instituto de Tecnología de Massachusetts para fundar el Consorcio de la **World Wide Web**, el W3C: una comunidad internacional dedicada al desarrollo de estándares abiertos de la *web*. Berners-Lee sigue siendo el director del W3C hasta el día de hoy.

Figura 22: Línea de tiempo para entender la creación de la *web*. **Fuente:** labSEAD-UFSC (2020).

En los años 80, había diferente información en diferentes computadoras, y el usuario necesitaba hacer *logon* en diferentes computadoras para acceder a ellas. Además, se tenía que aprender un programa diferente en cada computadora.

En su proyecto, Tim Berners-Lee pensó en una forma de resolver estos obstáculos, así como en la viabilidad de desarrollar aplicaciones mucho más amplias.

Figura 23: Accesibilidad digital. **Fuente:** Pixabay (2020).

Así, en octubre de 1990, el investigador estadounidense había escrito las tres tecnologías fundamentales que siguen siendo la base de la *web* actual, visibles en un navegador:

- **HTML** – HyperText Markup Language: **el lenguaje de marcas de la *web*.**
- **URL** – identificador uniforme de recursos: **una especie de dirección única utilizada para identificar cada recurso en la *web***.
- **HTTP** – protocolo de transferencia de hipertexto: **permite la recuperación de los recursos enlazados por la *web***.

Saber más

Tim Berners-Lee también escribió el primer editor de páginas *web/navegadores* "*worldwideweb.app*" y el primer servidor *web* http.

HTTP

HTTP son las siglas de Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto), es un protocolo de capa de aplicación para sistemas de información de hipermedia distribuidos y en colaboración que le permite a los usuarios comunicar datos en la World Wide Web.

> Como protocolo de solicitud-respuesta entre el cliente y el servidor, el HTTP ofrece a los usuarios una forma de interactuar con los recursos de la *web*, como los archivos HTML, mediante la transmisión de mensajes de hipertexto.

En este caso, el cliente es el navegador que se utiliza para acceder a Internet y el servidor es el que alberga un *site* o un dominio en la red. Los clientes HTTP suelen utilizar conexiones TCP (Transmission Control Protocol) para comunicarse con los servidores.

Figura 24: Al acceder a un *site*, hacemos la solicitud a través del protocolo HTTP. **Fuente:** labSEAD-UFSC (2020).

Para acceder a cualquier *site* de la red, cuando se pone la dirección de algún *site* en el campo de búsqueda del navegador, este envía una solicitud de acceso a una página. En respuesta, el servidor envía un permiso de acceso. Con ella, vienen los archivos que forman la página a la que el usuario quiere acceder, además de la información de hipertexto que hace otras peticiones para llevar al lector a otras páginas a través de *links*.

El HTTP utiliza métodos de solicitud específicos para realizar diversas tareas.

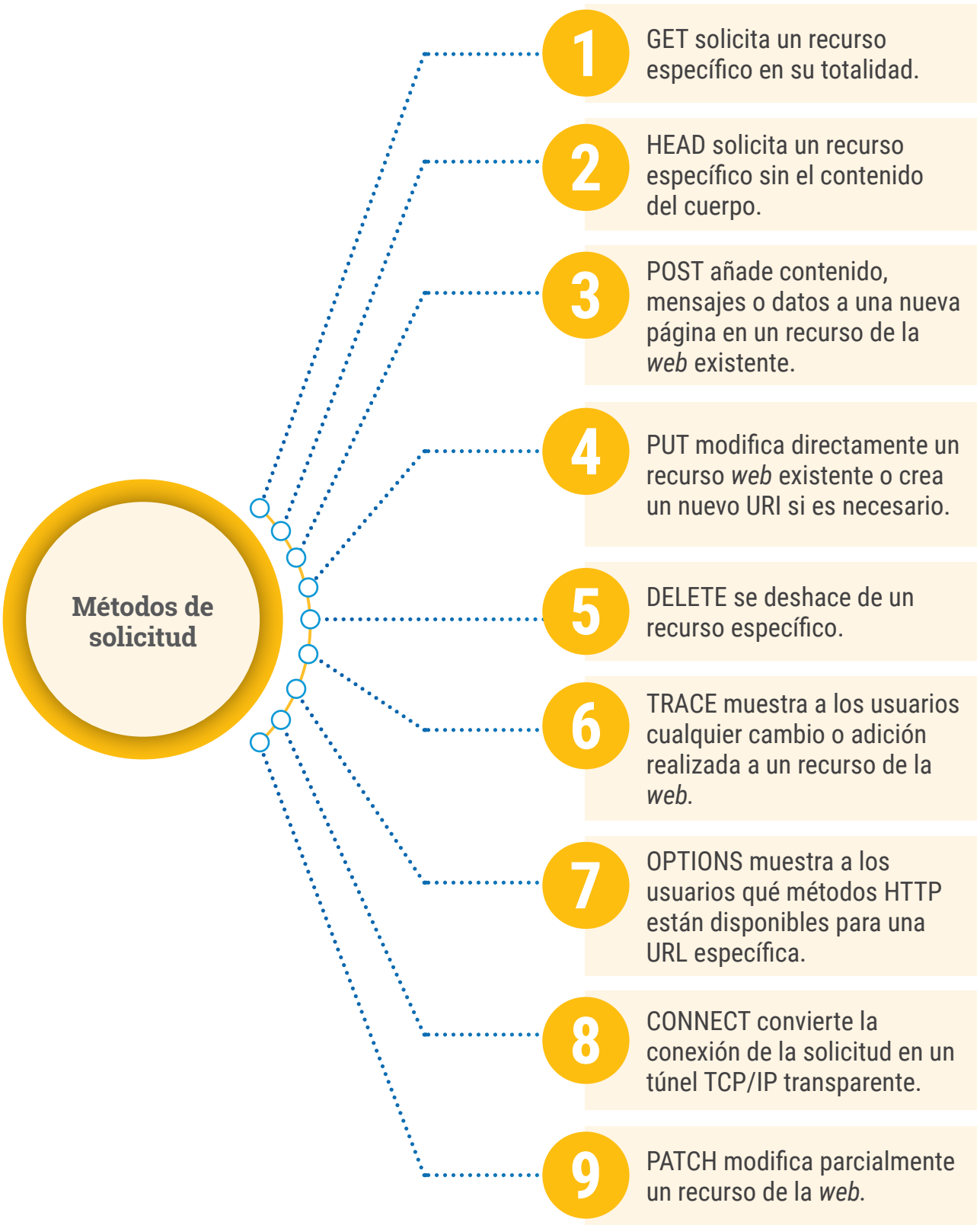


Figura 25: Solicitudes para realizar tareas.
Fuente: labSEAD-UFSC (2020).

Saber más

Todos los servidores HTTP utilizan los métodos GET y HEAD, pero no todos soportan el resto de estos métodos de solicitud.

El **HTTP** es el protocolo de transferencia de hipertexto más básico y se utiliza inicialmente para navegar por sitios de Internet. El protocolo **HTTPS** es el mismo, pero añade el término **"Seguro"**. Estos dos protocolos se utilizan para la misma transferencia de datos.

La diferencia básica entre los dos es la forma en que viajan los datos. Si los datos se transfieren a través de HTTP, viajan claramente y son accesibles para cualquiera que intercepte la comunicación.

El protocolo HTTPS, a su vez, utiliza una conexión segura mediante encriptación SSL y por lo tanto los datos viajan de forma segura de un lugar a otro. Observa, en la siguiente figura, cómo funciona el SSL.

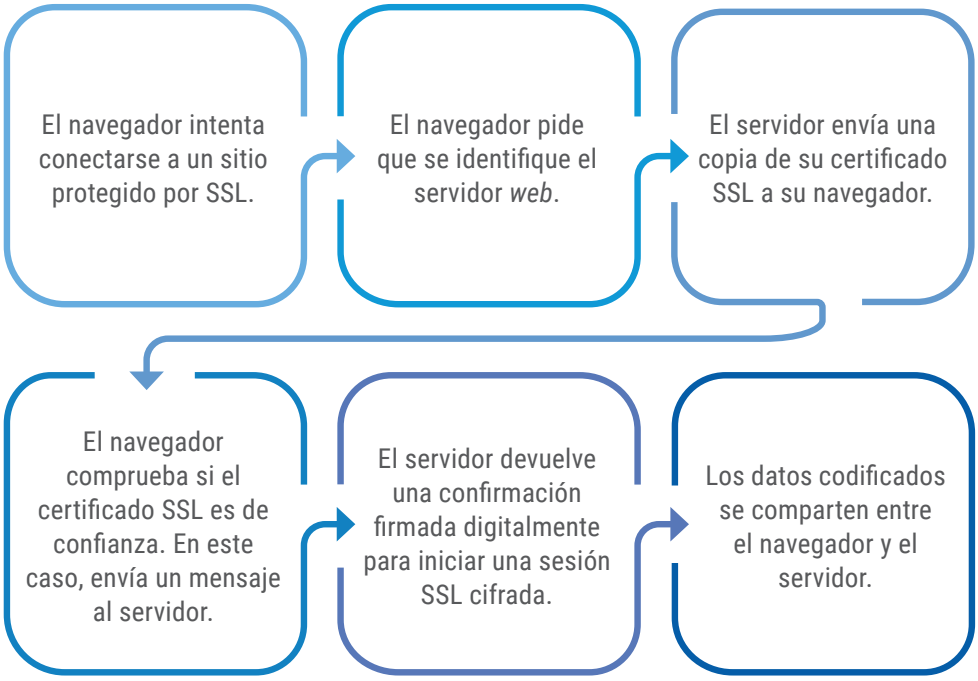


Figura 26: Pasos de la operación de encriptación SSL. **Fuente:** labSEAD-UFSC (2020).

De esta manera, un conjunto de datos del usuario está protegido por el protocolo de cifrado SSL durante el tráfico, incluyendo la dirección de *e-mail* y la contraseña, el número de la tarjeta de crédito, la cuenta bancaria y la información personal como el nombre, la dirección, la dirección de *e-mail*, el número de teléfono, etc.

En términos generales, los protocolos HTTP y HTTPS constituyen la base de cualquier intercambio de datos en la *web*. Debido a su extensibilidad, esta base de datos se utiliza no solo para buscar documentos de hipertexto, sino también imágenes y vídeos o para publicar contenidos en servidores, como los resultados de formularios HTML.

Figura 27: El HTTP es la base de las imágenes, los vídeos y las búsquedas de hipertexto. **Fuente:** Pixabay (2020).

En este sentido, su contribución al desarrollo de la *web* siempre ha sido muy importante, ya que ha consolidado históricamente los conceptos de "navegación", "site" y "búsqueda", elementos considerados atractivos para quienes viven la evolución de la "Era de la Información" en las últimas décadas.

La comunidad Tim Berners-Lee, fundada en 1994, produjo inicialmente algunas ideas revolucionarias que ahora se están extendiendo mucho más allá del sector de la tecnología.

Observe la siguiente figura.

Descentralización: no existe una autoridad central o un nodo de control de gestión y autorización para la publicación de contenidos en la *web*. Por lo tanto, hay una completa libertad contra la censura y la vigilancia indiscriminada.

No discriminación: significa igualdad para todos en cuanto a la calidad del servicio de conexión a la red. Este principio de equidad, también conocido como Net Neutrality (Neutralidad), está regulado en Brasil en el texto de la Ley 12.965/2014 (Marco Civil de Internet).

Diseño bottom-up (código abierto): toda la codificación aplicada en la *web* debe ser abierta, para que su desarrollo esté a la vista de todos, fomentando la máxima participación y experimentación.

Universalidad: para que cualquier persona pueda acceder al entorno *web* y participar efectivamente en él, todos los dispositivos implicados deben cumplir los mismos protocolos, sin importar las diferencias de *hardware*, el nivel de conocimientos técnicos, el lugar donde viven o sus creencias.

Figura 28: Resoluciones del W3C en la *web*.
Fuente: labSEAD-UFSC (2020).

La *web* tiene tres capas de desarrollo.

Figura 29: Tres capas de desarrollo de la *web*.
Fuente: labSEAD-UFSC (2020).

Cada una de las capas que vimos anteriormente está construida de forma independiente, lo que permite que la riqueza de la experiencia de los usuarios no sea destruida por una intervención en cualquiera de ellas.

Reflexionando sobre lo anterior, la diferencia entre Internet y la *web* parece clara. El Marco Civil de Internet define Internet de la siguiente manera:

> *Internet es el sistema compuesto por un conjunto de protocolos lógicos, estructurado a escala mundial para su uso público y sin restricciones, con el fin de permitir la comunicación de datos entre terminales a través de diferentes redes. (BRASIL, 2014).*

En general, podemos entender simplemente el **Internet** como la **"red de redes"** porque es capaz de conectar todas las redes de computadoras del mundo. Es la estructura a través de la cual se transfieren millones de *terabytes* de datos cada día entre los servidores y las computadoras personales, *smartphones*, *tablets*, consolas, televisores y varios otros dispositivos interconectados, siempre en constante expansión.

La World Wide Web, también conocida por seguir la **WWW** o simplemente el término *web*, puede entenderse como la parte lógica de esta gran red, también llamada "world web". De manera sencilla, la *web* puede definirse como el contenido transferido por Internet a través de las aplicaciones disponibles, lo que hace que esta experiencia sea "sensitiva". De modo simples, pode-se definir a *web* como o conteúdo transferido pela Internet através de aplicações disponíveis, o que torna essa experiência "sensitiva".

Clase 7 – Concepto y Características del Ciberespacio

CONTEXTUALIZANDO...

La *web* ha provocado un cambio significativo en la forma en que usamos Internet. A través de la *web*, tenemos el poder de comunicarnos y crear interfaces o entornos virtuales que permitan la integración. Desde esta perspectiva, este ideal de interacción se ha ido elaborando cada día más, con la interfaz humano-computadora, llevada a cabo mediante estructuras multimedia, en las que el *feedback* y la retroactividad habilitados por la cibernética se han hecho más adecuadas para la sensibilidad e inteligibilidad humana. Estamos hablando de la creación del **ciberespacio**, que será el tema de esta clase.

¡Continúa tus estudios y compruébalo!

USUARIOS DE INTERNET

Cada vez más, la tecnología permite la experiencia de "estar ahí" para el usuario que navega en *websites*. La vieja idea de crear "vida" en otro sustrato, hoy en día se materializa a través de la fusión entre la imagen real y la virtual, obtenida por las investigaciones realizadas con la tecnología de la realidad aumentada y el desarrollo gráfico, técnica que permite ver el mundo real con algunos objetos virtuales insertados en él, es decir, es la mezcla entre lo real y lo virtual.

Con la perspectiva de incluir al usuario en una participación activa en los *websites*, se apreció la idea de hacer de este usuario un coautor en la comunicación de estos *websites*.

Figura 30: Usuarios del ciberespacio. **Fuente:** Freepik (2020).

Este poder participativo y colectivo de los usuarios de Internet, incluidas las empresas inversoras, permitió su desarrollo exponencial basado en mejoras continuas del funcionamiento de los sitios y en el perfeccionamiento de los servicios ofrecidos. Cuanto más se asemeja la experiencia digital al mundo físico, más atractivo se vuelve el entorno, que se convierte en una invitación para un gran número de usuarios.

A mediados de 1984, William Gibson concibió la ficción de un espacio virtual compuesto de computadoras y usuarios conectados a una red mundial, que Gibson denominó ciberespacio.

Lo que vemos hoy es exactamente la creación de ambientes que simulan la vida real, siendo espacios que no existen físicamente, sino que están construidos virtualmente.

Saber más

El origen del término *ciber* se deriva del griego *kybernetes* y de su correlacionado vocablo latino *gubernator*, que significan el arte de pilotear o gobernar una náutica.

Observa la historia completa del origen del término en el *link* https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/ciber/1268.

La expresión deriva de los estudios sobre cibernética inaugurados por Wiener y Rosenblueth en la primera mitad del siglo XX, los cuales tenían como objetivo el control de la comunicación del hombre con la máquina.

Actualmente, entendemos esta realidad de una forma mucho más amplia, donde la comunicabilidad es perceptible en los siguientes estándares.

Figura 31:
La evolución de la comunicación con la tecnología.
Fuente: labSEAD-UFSC (2020).

A pesar de las concepciones más filosóficas, organizativas, sociológicas, psicológicas o jurídicas, el ciberespacio puede conceptualizarse de diferentes maneras.

> El ciberespacio es la dimensión o el entorno construido artificialmente en las redes de computación de datos, donde hay presencia humana, representada en forma de entidad virtual, con la capacidad de interactuar con otros y con el propio entorno, a través de elementos gráficos, textuales o realidades artificiales.

El concepto anterior se construyó a partir de las principales características del ciberespacio. Observa cómo se pueden enumerar estas características en la figura siguiente.

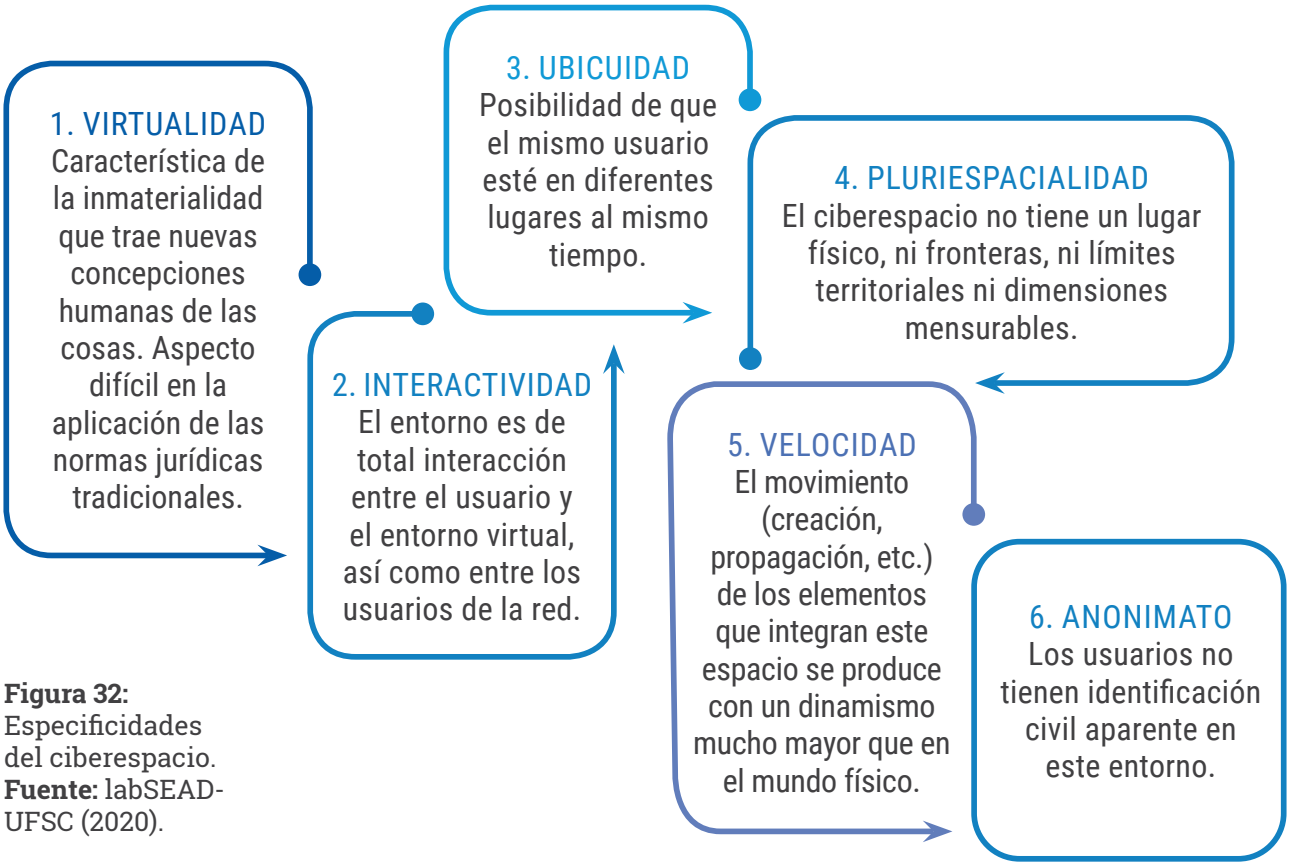


Figura 32: Especificidades del ciberespacio. **Fuente:** labSEAD-UFSC (2020).

Debido al anonimato, en Brasil hay, a menudo, conflictos de intereses protegidos constitucionalmente en la Carta Magna:

> *Todos son iguales ante la ley, sin distinción alguna, garantizando a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes [...].*
>
> *IV - la manifestación del pensamiento es libre y el anonimato está prohibido. (BRASIL, 2020, traducción nuestra).*

En una visión minimalista y estrictamente tecnológica, el ciberespacio sería la infraestructura técnica constituida por el conjunto interconectado de redes de información, públicas y privadas, incluido Internet.

En esta perspectiva, se incluirían todos los enlaces físicos y protocolos de control de las comunicaciones, así como los

sistemas informáticos, entendidos en sentido amplio, tanto para fines generales como para usos específicos e incorporados, además de los datos vinculados y almacenados a ellos.

Figura 33: El ciberespacio es la estructura de conexión de las redes. **Fuente:** Pixabay (2020).

Cabe señalar que, paralelamente al desarrollo de la *web*, la ingeniería y la informática presentaron importantes avances en las esferas de los gráficos por computadora y la realidad virtual, impulsados por el mercado de los *games*, que contribuyeron significativamente a la construcción de los denominados entornos cibernéticos.

Referencias

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 jul. 2020.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 jul. 2020.

CASTELLS, M. **A galáxia da internet**: reflexões sobre internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

FLATICON. [*S.l.*], 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 3 jul. 2020.

FEBRABAN. **Pesquisa FEBRABAN de Tecnologia Bancária 2019**. São Paulo: Federação Brasileira de Bancos, 2019. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 2 jul. 2020.

HOLODNY, E.; KIERSZ, A. CHART: How popular social networks stack up against the biggest countries in the world. **Business Insider**. Nova York, 3 fev. 2016. Disponível em: https://www.businessinsider.com/social-media-users-and-country-populations-2016-2. Acesso em: 3 jul. 2020.

KUROSE, J.; ROSS, K. **Redes de Computadores e a Internet**: uma abordagem top-down. 6. ed. São Paulo: Addison Wesley, 2013.

LÉVY, P. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2010.

PIXABAY. [*S.l.*], 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 2 jul. 2020.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 2 jul. 2020.

WIKIPEDIA. [*S.l.*], 2020. Disponível em: https://pt.wikipedia.org/wiki/Paul_Baran. Acesso em: 26 jul. 2020.

MÓDULO 2

LA CRIMINALIDAD EN EL CIBERESPACIO

Presentación

Como ya hemos visto, el ciberespacio se ha convertido en un área de intercomunicación social. Esta increíble revolución tecnológica significó el inicio de una nueva forma de comunicarse entre países y culturas de todo el mundo, contribuyendo decisivamente en el movimiento de globalización que se expandió en la década de 1990. Debido a esto, se ha desarrollado una simbiosis entre el mundo real y el virtual, interconectados hoy de tal manera, que cada vez es más difícil establecer límites.

Por lo tanto, observamos la preocupación de los países con el avance de nuevas modalidades de delitos cibernéticos, manteniéndose la evolución de esta práctica, por muchas décadas ya. En este módulo, comprenderemos la línea histórica de los delitos cibernéticos, además de conceptualizar, a través de sus características, los diversos tipos de delitos que pueden cometerse en el ciberespacio, y cómo son calificados jurídicamente.

OBJETIVOS DEL MÓDULO

Comprenderemos la historia y evolución del delito cibernético, además, de conceptualizar qué es en sí un delito cibernético. Igualmente, estudiaremos la clasificación otorgada a las diferentes modalidades de delitos cibernéticos, de acuerdo a sus características.

ESTRUCTURA DEL MÓDULO

- **Clase 1 –** Un Enfoque Histórico-Evolutivo de la Delincuencia Cibernética.
- **Clase 2 –** Concepto de Delitos Cibernéticos.
- **Clase 3 –** Clasificación de Delitos Cibernéticos.
- **Clase 4 –** Características de los Delitos Cibernéticos.
- **Clase 5 –** Principales Tipos de Delitos Cibernéticos.

Clase 1 – Un Enfoque Histórico-Evolutivo de la Delincuencia Cibernética

CONTEXTUALIZANDO...

En la segunda mitad del siglo XX, los países ya estaban preocupados por detener el avance de nuevas formas criminales, sobre todo, aquellos delitos que históricamente no eran comunes, tales como, delitos contra la propiedad jurídica no material, la propiedad intelectual, o delitos contra el honor y la intimidad de las personas.

Sin embargo, aunque esos delitos no dañaban los bienes corporales, sólo se materializaban después de una conducta cometida en el espacio físico. En relación con Internet, la posibilidad de relaciones múltiples ha dado lugar a la aparición de un nuevo tipo de delito, impulsado por la sensación de anonimato y libertad que la realidad virtualizada proporciona a sus usuarios.

En esta clase, haremos un análisis histórico de la delincuencia cibernética o, en otras palabras, entenderemos la evolución histórica del delito cibernético.

RELACIONES MÚLTIPLES EN EL CIBERESPACIO

El avance de la red de Internet y la popularización de los dispositivos celulares con conexión a la red atrajo a miles de usuarios al ciberespacio. usuários ao ciberespaço.

Figura 1: Mundo real y mundo virtual. **Fuente:** Pixabay (2020).

La construcción de este entorno colectivo, ampliado exponencialmente por la participación activa de miles de personas expresando sus ideas y siendo parte activa de estructuras cibernéticas, tales como plataformas y aplicaciones, sistemas ciber-físicos, así como *Internet of Things* (IoT), por ejemplo.

Figura 2: El ciberespacio es una creación colectiva. **Fuente:** labSEAD-UFSC (2020).

Así, observamos como esa producción de datos masiva, generó un nuevo modelo de negocios basado en el valor de la información.

> La recopilación insaciable por grandes compañías interesadas en descubrir las preferencias del consumidor, trajo consigo, un gran debate sobre la violación a la privacidad de las personas.

Lo mismo ocurre con la difusión de las llamadas “redes sociales” y aplicaciones de mensajería. Estas son interfaces ambiguas:

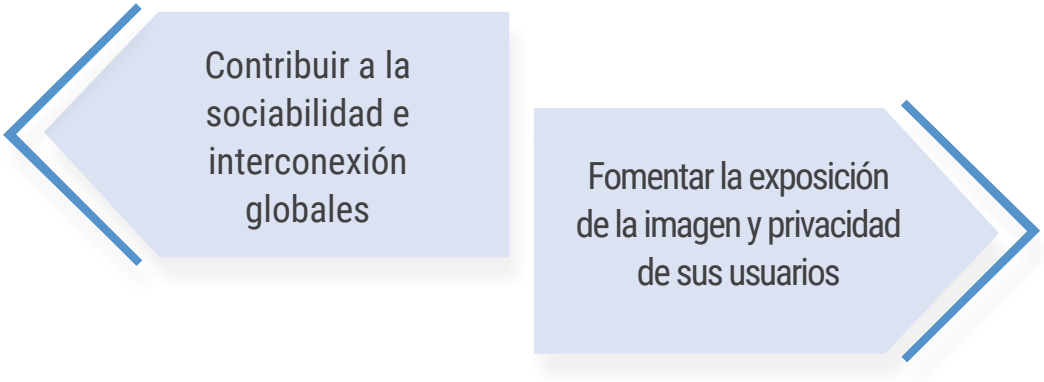


Figura 3: Acciones positivas y negativas que pueden surgir de las redes sociales. **Fuente:** labSEAD-UFSC (2020).

A menudo, los usuarios no se preocupan por los riesgos que corre su propia seguridad, cuando realizan publicaciones que revelan su paradero y patrimonio.

En estos espacios, la relevancia de una entidad virtual (perfil, cuenta, etc.) es directamente proporcional a cómo es presentada, lo que estimula la cultura de autopromoción. Ver:

Figura 4: Diferentes acciones que pueden originarse a partir de la autopromoción. **Fuente:** Freepik (2020), adaptado por labSEAD-UFSC (2020).

Las dos situaciones señaladas anteriormente, ejemplifican a una posible víctima y a un posible delincuente, respectivamente. Sin embargo, en ambos casos, por encima de sus intereses personales radica el deseo de notoriedad.

Aunado a ello, existe una tendencia migratoria al entorno virtual de los servicios más utilizados por el ciudadano, tanto estadales, como la banca o el comercio, ello también representa un factor determinante en una sociedad de riesgo.

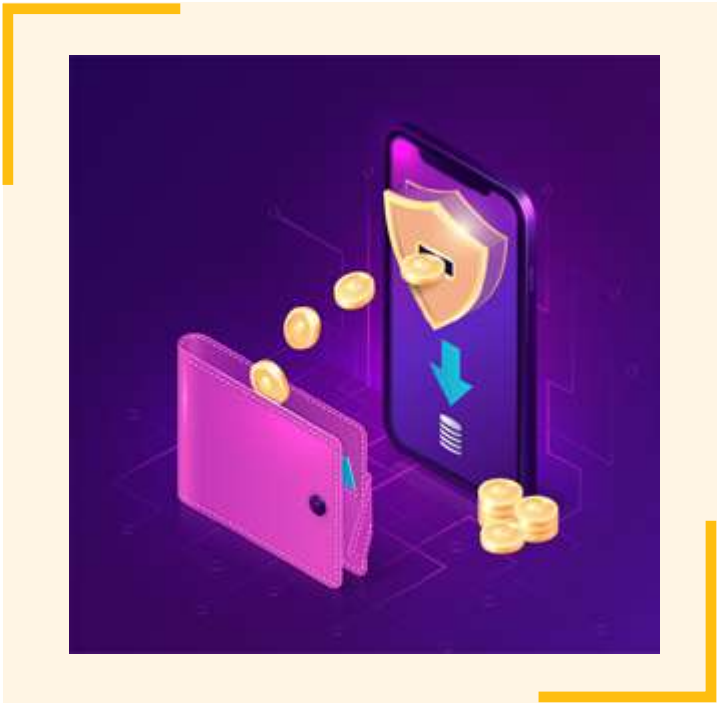


Figura 5: Servicios de *internet banking* han supuesto nuevos riesgos para el usuario. **Fuente:** Pixabay (2020).

Los proveedores de estas plataformas, condicionan sus acciones a las respuestas sobre datos personales y sensibles, introducidos por los usuarios. Este ejercicio, a su vez, es puesto en práctica todos los días en materia de seguridad, obligando al usuario a responderlas en toda red, entorno digital u archivos a los que desea acceder, teniendo que autenticarse a través de diversos procesos, como insertar contraseñas, biometría, etc.

> Esta realidad que abrió la posibilidad de relaciones múltiples ha dado lugar a la aparición de un nuevo tipo de delito, impulsado por la sensación de anonimato y libertad que la realidad virtualizada proporciona a sus usuarios.

Al virtualizarse como miembro de una red, las personas pueden asumir varias caras, recrear identidades falsas, enmascarar su propio origen y explotar las vulnerabilidades de otros usuarios con los que se relacionan bajo este perfil falso, actuando con el propósito deliberado de cometer actos ilícitos.

Figura 6: Los *hackers* usan el anonimato para cometer delitos cibernéticos.
Fuente: Pixabay (2020).

Teniendo en cuenta que la constante variación de hábitos y rutinas -que antes sólo podía apreciarse en el mundo real- ahora puede ser vigilado a través de aplicaciones en el entorno digital; la tendencia a esperar será hacia una concepción más amplia del fenómeno del crimen cibernético, si no existe un control efectivo del mismo.

> El escenario actual de **la criminalidad en el entorno virtual** puede ser controlado mediante **la virtualización de la propia delincuencia**, lo que implicaría un proceso de transformación, en el que todos los crímenes que hoy conocemos se extenderían en espacios virtuales o cibernéticos, debido a la inminencia de un mundo cada vez más digital.

La verdad es que, cada vez se hace más claro, que no solo se cometen crímenes contra el honor y el patrimonio en el entorno cibernético, sino que también existen crímenes cibernéticos capaces de afectar la salud, integridad física e incluso la vida de las personas.

En algunos países, los dispositivos capaces de proporcionar la supervivencia de pacientes en los centros de salud, son controlados por sistemas. Un ataque capaz de interrumpir el funcionamiento de estas máquinas puede configurar un homicidio múltiple, considerando las probabilidades de que sea detectado y la proporcionalidad del ataque.

Figura 7: Ciberseguridad. **Fuente:** Freepik (2020), adaptado por labSEAD-UFSC (2020).

Resumiendo la evolución del **crimen cibernético** en el mundo, destacamos:

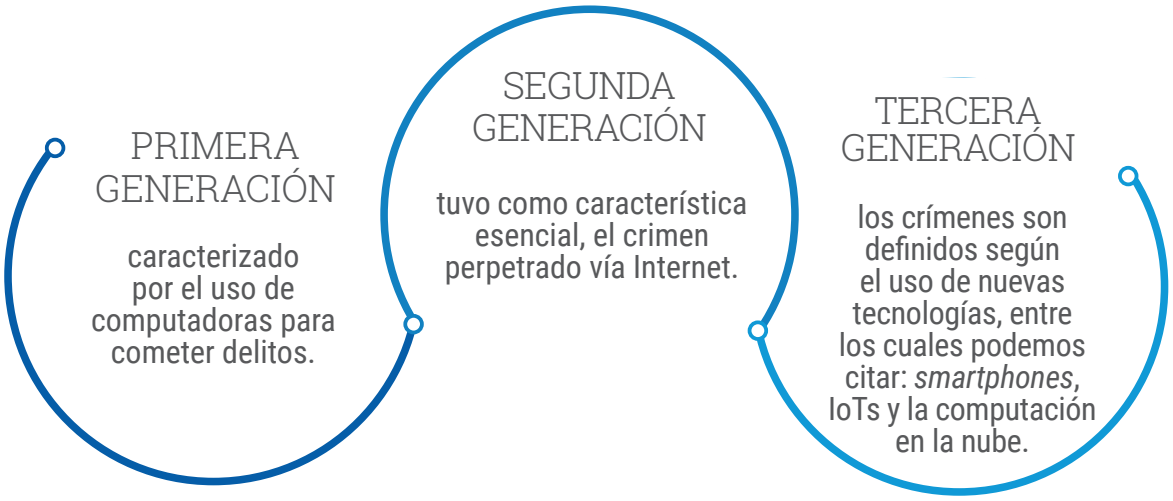


Figura 8: Resumen de la evolución del delito cibernético.
Fuente: labSEAD-UFSC (2020).

Esta historia se puede entender a través de la cronología de acontecimientos notables que se sucedieron entre sí desde la década de 1970 en adelante, que se muestran a continuación.

Década de 1970

Phreaker es el nombre que reciben los crackers telefónicos.

1971 – John Draper, un ***phreak*** telefónico, descubrió que el silbato que era entregado como premio en las cajas de cereales Cap'n Crunch, emitía los mismos tonos de los computadores responsables por el intercambio de líneas telefónicas en la época. Construyó una "caja azul" con el silbato, lo que permitía, emular al computador y hacer llamadas telefónicas de larga distancia gratuitas, posteriormente publicó instrucciones sobre cómo hacerlo.

Saber más

Phone phreak es un término utilizado para describir programadores de computadoras obsesionados con redes de telefonía, las cuales sin dudas, son la base de la red informática moderna.

1973 – Un operador de un banco local de Nueva York, utilizó un computador para malversar más de dos millones de dólares.

Década de 1980

1981 – Ian Murphy, conocido por sus seguidores como el Capitán Zap, fue la primera persona condenada por un delito cibernético en la historia. Irrumpió en la red de AT&T y cambió el reloj interno para cobrar -en los horarios más concurridos- tarifas solamente exigidas fuera de este período.

Figura 9: Invasión en la red de datos. **Fuente:** Freepik (2020), adaptado por labSEAD-UFSC (2020).

Su sentencia consistió en proporcionar 1.000 horas de servicio comunitario, además de dos años y seis meses de libertad condicional.

1982 – Elk Cloner, un virus, fue diseñado como una broma por un niño de 15 años. Este hecho se destacó por ser uno de los primeros virus en dejar un sistema operativo original y propagarse fácilmente. Atacó los sistemas operativos Apple II y se propagó a través de disquetes infectados.

1988 – Robert T. Morris Jr. lanzó un *worm* (un programa autorreplicante, que difiere de un virus pues no necesita de otro para propagarse) en la desaparecida *Advanced Research Projects Agency Network* (ARPANET). Este programa se puede diseñar para realizar acciones maliciosas después de infectar un sistema, como eliminar archivos de dicho sistema o enviar documentos por *e-mail*, por ejemplo.

Figura 10: Acceso a archivos confidenciales. **Fuente:** Freepik (2020).

El *worm* lanzado por Morris infectó más de 600.000 computadoras conectadas en red. Morris fue sentenciado a pagar una multa de US$ 10.000 (diez mil dólares) y a 3 años de libertad condicional.

1989 – Se conoce el primer caso de *ransomware* (secuestro de datos encriptados por programas maliciosos) a gran escala.

> El virus fue presentado como una prueba del virus SIDA y, una vez descargado, mantenía los datos informáticos secuestrados a cambios de US $ 500 dólares (quinientos dólares).

También en 1989, otro grupo de personas fue arrestado por robar datos del gobierno estadounidense y del sector privado, para venderlos a la extinta KGB.

Década de 1990

1994 – Un estudiante en el Reino Unido, ideó un ataque informático para invadir el programa nuclear de Corea, la NASA y otras agencias de Estados Unidos utilizando solo un computador personal y un programa de *blueboxing* encontrado *on-line*.

1995 – Surgieron macrovirus escritos en lenguajes informáticos que fueron hallados encriptados en aplicaciones. Estos macros lenguajes se ejecutan cuando se abre la aplicación infectada, esto puede ser, un documento de texto, hojas de cálculo, archivos PDF e incluso imágenes. Esta manera resulta fácil para *hackers*, pues solo necesitan insertar el *malware (malicious software)* en los sistemas operativos de las víctimas.

Figura 11: Los cibe ataques pueden ser realizados por varias personas. **Fuente:** Pixabay (2020).

1999 – El "Virus Melissa" fue liberado y se convirtió en una de las infecciones más potentes hasta la fecha, resultando históricamente, en una de las primeras condenas para alguien que escribió un *malware*. El "Virus Melissa" fue un macrovirus desarrollado con la intención de invadir las cuentas y enviar *e-mails* masivamente. El creador de este virus fue acusado de causar más de USD $ 80 (ochenta millones de dólares) en daños a las redes informáticas y, por esta razón, sentenciado a 5 años de prisión.

Años 2000

2000 – A partir de esa década, el número y los tipos de ataques *on-line* han aumentado exponencialmente. Los ataques para la denegación de servicios (DDoS) se han efectuado varias veces en contra compañías como: AOL, Yahoo!, Ebay y muchas más.

Figura 12: Aumento de la conexión desde la década de 2000. **Fuente:** Pexels (2020).

Este ataque no es una invasión del sistema, sino una técnica que busca hacer que las páginas web no se encuentren disponibles en la red, debido a una sobrecarga.

Figura 13: DDoS hace que la página web no esté disponible. **Fuente:** Pixabay (2020).

Para ello, el atacante efectúa un comando en cientos de máquinas infectadas y controladas, de modo que puedan acceder simultáneamente a la misma página web. Ese año, el famoso virus *I love you* se extendió a través de Internet.

2003 – SQL Slammer se convirtió en el *worm* más rápido de la historia. Infectó servidores SQL y creó un ataque de denegación de servicios (DDoS) que afectó a 75.000 equipos en menos de 10 minutos.

2006 – Un *hacker* logró invadir el sistema de registro automatizado de varias instituciones educativas estadounidenses, y decidió compartir toda esa información con terceros, incluyendo las vulnerabilidades que le permitieron acceder a los sistemas de las universidades. El método finalmente se deshabilitó de Internet, pero no se encontró al culpable.

2008 – Ataques *hackers* fueron hechos desde una estación terrestre contra los sistemas de control satelitales estadounidenses. Entre los posibles autores se encuentra un escuadrón militar chino.

> En el caso de los satélites Landsat-7 y Terra AM-1, los cuales eran controlados por la NASA, y utilizados para la predicción meteorológica. Durante ese mismo año, por acción de un *malware* diseñado para redireccionar el tráfico de los mismos, los *hackers* impactaron a millones de usuarios en todo el mundo.

Cerca de 26.000 sitios web fueron utilizados por un grupo de *hackers* para redireccionar su tráfico hacia su propio código en JavaScript. El código malicioso estaba oculto en los sitios web, totalmente invisible para los usuarios, pero que se podía activar por *hackers* en cualquier momento. Otra acción en este sentido fue atribuida a un miembro del grupo de *hackers* Krygenics, que fue capaz de acceder a los registros de Comcast.net, gestionados por la empresa Network Solutions. Así, las personas que intentaron acceder a sus *e-mails* en la página Comcast fueron redireccionadas automáticamente a la página del *hacker*.

2010 a 2020

2010 – Un *malware* llamado Stuxnet, descubierto por una empresa de seguridad bielorrusa, fue especialmente diseñado para atacar al SCADA, que es el sistema operativo utilizado para controlar las centrifugadoras nucleares de Irán. Este fue uno de los primeros ataques a sistemas ciberfísicos en la historia.

2011 – La compañía Sony ha tenido su espacio de juegos, llamado PlayStation Network, invadido.

Figura 14: La piratería informática de sistemas es un delito cibernético. **Fuente:** Freepik (2020).

Hackers no identificados penetraron en la red, irrumpiendo la conexión para robar datos personales de más de 77.000 usuarios del servicio, lo que llevó a la compañía a atender muchas quejas e incluso múltiples demandas.

2014 – La compañía Yahoo! confirmó la invasión en su sistema por parte de un *hacker*, lo cual comprometió la seguridad de 500 millones de usuarios. En el mismo año, Sony Pictures, la división cinematográfica de la marca Sony, también fue atacada.

Figura 15: Fuga de información. **Fuente:** Pexels (2020).

No tardó mucho tiempo para que sus redes fueran violentadas nuevamente, esta vez, por un grupo de *hackers* conocidos como *Guardians of Peace* (Guardianes de Paz), quienes filtraron información sobre empleados y ejecutivos del estudio.

2016 – Los ciberdelincuentes han decidido ejecutar un ataque colosal de DDoS contra Dyn, una compañía estadounidense que opera servicios DNS. Sus sistemas no soportaron la gran demanda exigida y acabó siendo interrumpido su funcionamiento, dejando fuera de servicio a clientes importantes como **Amazon**, **Netflix**, **PayPal**, **Spotify**, **Tumblr**, **Twitter**, **Xbox Live** y **PlayStation Network**.

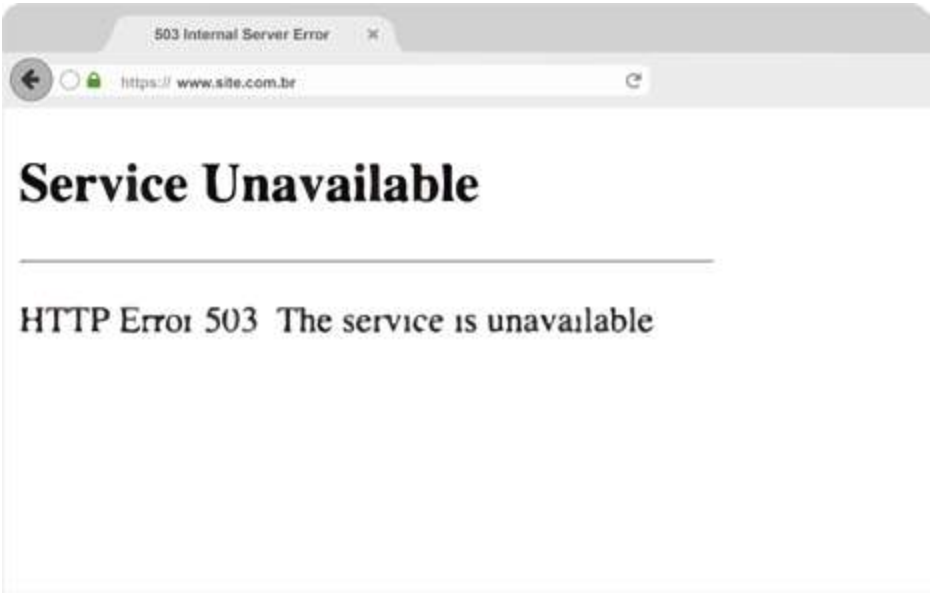


Figura 16: Páginas fuera de servicio. **Fuente:** labSEAD-UFSC (2020).

Las empresas de medios digitales y tiendas en línea en los Estados Unidos también quedaron fuera de servicio. Este incidente se conoció como "**el apagón del *Internet* Estadounidense**" y se atribuyó a *hackers* de Corea del Norte, considerando que una de las peticiones que se hicieron para cesar el ataque, fue que la compañía cancelara el estreno de "The Interview", una película de comedia que satirizaba a Kim Jong-un, líder supremo del país.

2017 – En mayo, más de 230.000 sistemas alrededor del planeta fueron secuestrados por un *malware* llamado WannaCry. Este virus, de hecho, era un *ransomware*, que es un *malware* que logra **encriptar** los archivos dentro un computador, para condicionar a la víctima del ataque, a realizar un pago a los criminales con el fin de desencriptar los archivos.

Encriptar: modificar una información en código secreto (cifrado), que solo puede ser leído por aquellos que tienen la clave para descifrarlo. Sinónimo de Codificar; Cifrar.

2018 a 2020 - As instâncias de *hacking*, roubo de dados e infecções por *malware* disparam.

> El número de registros robados y máquinas infectadas se eleva a millones; cantidad de daño infligido, a miles de millones. La tecnología móvil trae consigo la llegada de nuevas formas de ataques y delitos cibernéticos.

Posterior a que el gobierno chino fuese acusado por las invasiones recientes en sistemas gubernamentales de Estados Unidos, invasiones como el ataque a los sistemas de control por satélite de 2008 y otro más, los medios internacionales comenzaron a utilizar la frase **"Guerra Cibernética"**.

LOS DELITOS CIBERNÉTICOS EN BRASIL

Brasil no es inmune a esta realidad: se posiciona como el segundo país del mundo con mayores pérdidas económicas debido a ciberataques, únicamente detrás de China, que ocupa la primera posición. El número de ciberataques ocurre debido al gran número de personas que permanecen conectadas a Internet.

Figura 17: Ciberataques en Brasil. **Fuente:** labSEAD-UFSC (2020).

En estos países, el crecimiento de la accesibilidad a la red es proporcional al índice de adquisición de dispositivos móviles. La primera vez que la cantidad de dispositivos conectados excedió el número de habitantes en Brasil fue en 2018. Esta realidad tiene un impacto decisivo en el aumento de la delincuencia en el entorno cibernético.

Saber más

Según la Oficina de Seguridad Institucional (GSI) de la Presidencia de la República, en 2019, setenta millones de brasileños fueron víctimas de delitos cibernéticos, causando una pérdida al país de más de veinte mil millones de dólares.

Para obtener más información, ingresa al *link*:

https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia.

Registramos el aumento de una amplia lista de crímenes dentro el país, incluyendo, por ejemplo:

Figura 18: Principales delitos denunciados frente al Sistema de Seguridad Nacional. **Fuente:** labSEAD-UFSC (2020).

Estas son las principales modalidades de delitos cibernéticos, denunciados ante las fuerzas que integran la Seguridad Pública en Brasil.

Además de estos registros, las empresas responsables de proporcionar seguridad de datos y responder ante incidentes de tal índole en corporaciones, también han proporcionado datos estadísticos que indican, en general, el aumento en el número de estos ataques realizados dentro del país, destacando los casos de otros *malwares*. ¡Conoce más a continuación!

Figura 19: Nuevos delitos cibernéticos.
Fuente: labSEAD-UFSC (2020).

El Internet de las Cosas, de la misma manera, ya demuestra cómo se ampliará el espectro de oportunidades para delincuentes cibernéticos en los próximos años.

Los ataques ya son recurrentes en cámaras, generalmente muy baratas, que tienen sensores, como el micrófono, capaces de transmitir datos a otras empresas y a los cuales se puede acceder de forma remota. Además, la mayoría de las personas no cambian las contraseñas que vienen de fábrica y obedecen a un patrón fácilmente detectable, generando así una gran vulnerabilidad, fácilmente aprovechada por los atacantes de la red.

Clase 2 – Concepto de Delitos Cibernéticos

CONTEXTUALIZANDO...

¿Cómo conceptualizar los delitos cibernéticos? Es posible que hayas escuchado al menos algunos de estos términos: **delitos digitales, delitos virtuales, crímenes electrónicos, delitos electrónicos, delitos informáticos, delitos telemáticos.**

En esta clase, vamos a entender cuál es la definición de delito cibernético y qué dicen los autores acerca de la terminología correcta de este tipo de delito.

¿QUÉ ES EL CRIMEN CIBERNÉTICO?

¿Qué es, después de todo, un crimen cibernético?La comprensión más obvia, basada en todas las construcciones doctrinales desarrolladas hasta ahora, es que se trata de un término que abarca las posibles tipologías criminales que pueden ocurrir en el ciberespacio.

Como vimos, el surgimiento y desarrollo de esta nueva dimensión -paralela de la experiencia humana- trajo consigo nuevos fenómenos sociales que eran preexistentes, incluyendo el de una nueva cultura criminal.

> Internet simplemente promovió la popularización del ciberespacio como un ámbito de intercomunicación social, a través de interacciones y nuevos cimientos para la sociedad, pues volvió accesible el contacto entre personas que permanecían muy distantes entre sí, considerando la realidad del entorno físico. Por otro lado, estableció un nuevo espacio muy atractivo para los delincuentes.

Según la doctrina, el crimen puede ser conceptualizado bajo tres enfoques: el aspecto material, el aspecto legal o formal y el aspecto analítico. Analicemos tales aspectos:

Aspecto del material	Aspecto jurídico o formal	Aspecto analítico
El delito es toda acción humana que endurece o expone a peligro un bien jurídico de un tercero que, debido a su pertinencia, merece protección penal.	Se considera delito todo delito penal al que la ley castiga con pena de prisión o detención, de conformidad con el art. 1º de la Ley de Introducción al Código Penal.	En Brasil predomina la teoría tripartita, que considera el hecho típico, ilícito y culpable como un delito.

Figura 20: Aspectos que caracterizan la delincuencia. **Fuente:** labSEAD-UFSC (2020).

Para una conceptualización del crimen o delito cibernético, bajo cualquiera de los enfoques, es importante destacar que el aspecto principal que caracteriza dicho fenómeno y que le diferencia de otros delitos, es invariable: **el medio por el cual se produce el delito**.

La expresión delito cibernético se utilizó a finales de la década de 1990, cuando Internet comenzó su expansión mundial.

Un grupo de representantes de las naciones del G8, después de una reunión en Lyon (Francia), acogió el término para describir todos los tipos de delitos perpetrados en Internet o en nuevas redes de telecomunicaciones. Años más tarde, la Convención sobre el Delito Cibernético (2001), conocida mundialmente como Convención de Budapest, firmó en su preámbulo un concepto de delito cibernético.

> Rossini (2004) lo configuró como actos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos informáticos, así como el uso fraudulento de estos sistemas, redes y datos informáticos.

Esta visión centrada en el bien jurídico constituido por "la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos informáticos" (ROSSINI, 2004) ha sido acogida por algunos académicos. Asimismo, hay quienes restringen esta definición a delitos cometidos contra sistemas y computadoras.

A continuación, citamos los siguientes conceptos:

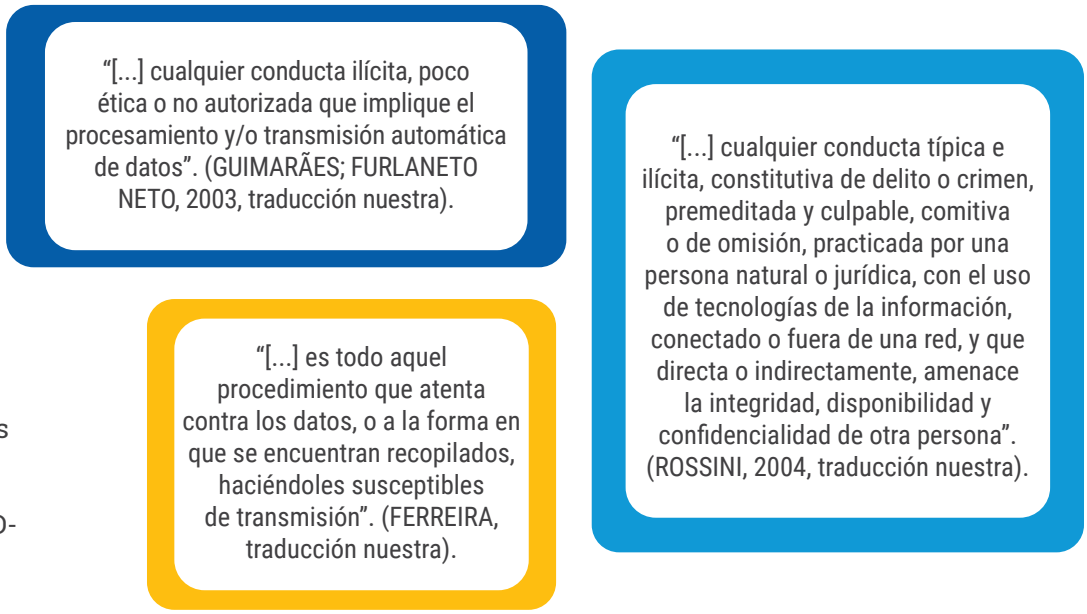


Figura 21: Conceptos de delitos y ataques contra sistemas informáticos.
Fuente: labSEAD-UFSC (2020).

Dada la evidente complejidad del ciberespacio, los puntos de vista anteriores se consideran conceptualmente restrictivos.

La esencia parece estar en la comprensión de que este fenómeno corresponde a una categoría más amplia de comportamientos que corresponden a los considerados típicos y que se perpetran en el espacio virtualizado, fuera de la dimensión física o natural, aunque allí se generen efectos.

> Por esta razón, se considera que la mejor definición de delito cibernético es la que trata el fenómeno, simplemente, como **crímenes ocurridos en el entorno cibernético**.

En este sentido, el delito o crimen cibernético, se configura cuando se manifiestan comportamientos delictivos practicados en el ciberespacio, en los que la esencia del daño no podría haber ocurrido en ningún otro espacio. Desde esta perspectiva, cualquier comportamiento delictivo que se produzca en el espacio o el entorno cibernético es admitido como delito cibernético, incluyendo los tipos de delitos ejecutados tradicionalmente sin necesidad de ser materializados en el entorno virtual, pero que efectivamente hoy también evolucionaron a la dimensión tecnológica.

Para denominar este fenómeno social, algunos autores usan otras terminologías:

Figura 22: Expresiones utilizadas para caracterizar el delito o crimen cibernético. **Fuente:** labSEAD-UFSC (2020).

Dada la alusión directa al espacio cibernético, la expresión **delito cibernético** parece ser la más apropiada para el contexto, sin descuidar el valor terminológico de otras expresiones utilizadas por sus autores.

Clase 3 – Clasificación de Delitos Cibernéticos

CONTEXTUALIZANDO...

Con el avance de la tecnología, se propulsó la invención de nuevos delitos cometidos en el ciberespacio.

En esta clase, vamos a aprender acerca de las diferentes formas de clasificar el delito o crimen cibernético.

FORMAS DE CLASIFICAR LOS DELITOS CIBERNÉTICOS

Aunque el crimen cibernético se concibe aún como algo novedoso, es importante resaltar el importante trabajo de los autores, para crear una doctrina especializada sobre el tema. Aún así, hay divergencias con respecto a conceptos y métodos sobre el objeto.

En este sentido, en lo que respecta a la **taxonomía**, también encontramos diferentes enfoques, especialmente en lo que respecta a las formas de clasificación de los delitos cibernéticos.

Taxonomía es la ciencia o técnica de clasificación.

Figura 23: Delitos cibernéticos.
Fuente: Pixaby (2020), adaptado por labSEAD-UFSC (2020).

Los académicos eligieron diferentes ámbitos para establecer sus clasificaciones, la imagen a continuación, representa brevemente tales formas de clasificación:

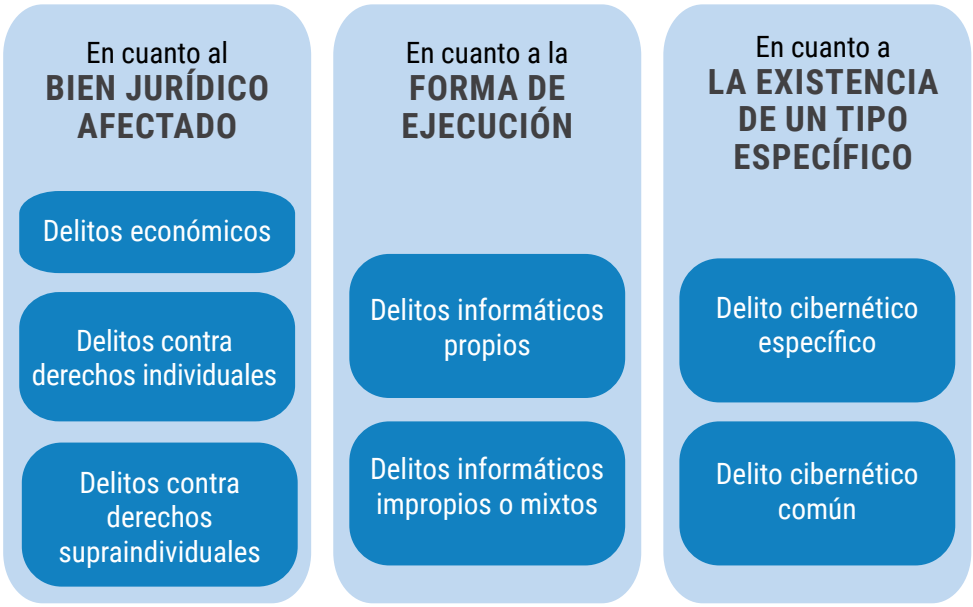


Figura 24: Clasificación de los delitos cibernéticos.
Fuente: labSEAD-UFSC (2020).

¡Estudiemos con más detalle cada uno de ellos!

Respecto al bien jurídico afectado

Esta clasificación fue presentada por Ulrich Sieber y considera el valor o interés de alguien amparado por la ley, en el cual se basa el Derecho Penal para elaborar normas penales incriminatorias. Desde esta perspectiva, los delitos se clasifican como: económicos, contra derechos individuales y contra derechos supraindividuales

Delitos económicos

Son delitos que atentan contra el patrimonio jurídico de carácter patrimonial. En este ámbito, están contemplados delitos clásicos como el hurto -evidentemente con sesgo tecnológico- y nuevas modalidades penales, como el *ransomware*.

Figura 25: Fraude económico. **Fuente:** Pixabay (2020).

Delitos contra derechos individuales

Esta categoría corresponde a los ataques contra bienes jurídicos individuales y no patrimoniales por medios digitales, tales como el honor y la libertad individual.

Delitos contra derechos supraindividuales

Son delitos que afectan a bienes jurídicos cuya titularidad es de carácter no personal, afectando a un determinado grupo de personas o a toda la comunidad, sin perder la referencia individual.

Figura 26: Víctimas de crímenes cibernéticos contra el honor. **Fuente:** Pixabay (2020).

Entre los ejemplos cabe citar los delitos motivados por el odio contra las etnias y racismo perpetrado en Internet.

En cuanto a la ejecución

Esta clasificación, iniciada por Hervé Croze e Yves Bismuth, es la más encontrada en libros y artículos científicos sobre el tema. Entendiendo su taxonomía, es tomado en consideración el **instrumento tecnológico** y el **medio dónde es cometido el crimen.** Veamos a continuación la forma en la que son clasificados los delitos.

Figura 27: Diferencias entre los delitos informáticos.
Fuente: labSEAD-UFSC (2020).

Ahora pasemos a la clasificación, en cuanto a la existencia de tipos específicos.

Existencia de tipos específicos

Esta clasificación se basa en la existencia o no, de una regla específica para una determinada conducta, describiendo el delito como universal, pero que cuenta con ciertas características que **lo convierten, o encajan, en un tipo de delito cibernético.** Con base a estas ideas, Roberto Chacón de Albuquerque divide las modalidades criminales en dos grupos:

Delitos cibernéticos específicos

Se refiere a la conducta practicada exclusivamente en el ambiente cibernético y que el legislador penal le establece como un tipo específico, para calificarlo como criminal.

Figura 28: Invasión de dispositivos tecnológicos.
Fuente: Freepik (2020).

Se configura cuando ocurre una invasión en dispositivos tecnológicos, de acuerdo con el Art. 154-A del Código Penal de Brasil.

Delitos cibernéticos comunes

Se refiere a todos los delitos susceptibles de ocurrir en el entorno cibernético, pero no excluyentemente por fuerza de ley. Se trata también de delitos se consuman en el medio físico o natural. Podemos encontrar aquí los delitos contra el honor, o delitos contra el patrimonio.

Nuevo delito cibernético

Recientemente, se incorporó al Código Penal de Brasil el Art. 218-C, que tipifica como delito la "revelación de una escena de violación de personas y/o de personas vulnerables, cualquier escena sexual o pornográfica sin autorización de las personas involucradas".

Figura 29: Los delitos cibernéticos también están contemplados en el Estatuto de la Niñez y la Adolescencia.
Fuente: Pixabay (2020).

Aunque esta tipificación es entendida como un nuevo delito cibernético, se trató de la formalización meramente de una conducta criminal que se venían conociendo como “venganza digital” (propagación de archivos y/o contenido íntimo por motivo de venganza), aunque la legislación ha dejado abierta la posibilidad de que el delito sea cometido en un entorno no cibernético. La intención ha sido, detener un delito cibernético alarmantemente común.

Clase 4 – Características de los Delitos Cibernéticos

CONTEXTUALIZANDO...

Los delitos cibernéticos tienen características específicas, y aquellos que cometen estos delitos terminan apelando a los vacíos legales, para cometer sus crímenes. Por ejemplo, la posibilidad de ser usuarios anónimos en Internet contribuye a la perpetuación del crimen cibernético, en este sentido, el anonimato es una de las posibilidades permitidas del ciberespacio.

En esta clase, estudiaremos otras características también presentes en el delito cibernético.

PRÁCTICAS ILÍCITAS EN EL CIBERESPACIO

Como ya vimos en otros momentos, el delito cibernético presenta elementos distintivos de la delincuencia común. No se trata sólo de conductas ilegales llevadas a cabo mediante el una máquina, conectada o no, con alguna red.

> La complejidad de los espacios envueltos, se refleja en la gran diversidad de delitos abarcan desde la manipulación de cajeros bancarios hasta la piratería de programas informáticos, pasando por abusos en sistemas de telecomunicaciones y llegando a las capas más profundas, como la *Deep Web*, donde se ve la propagación de mensajes de odio y hasta el intercambio de pedofilia.

Los ataques generalmente ocurren en el ciberespacio, apuntando a los más diversos objetivos, y aplicando una infinita variedad de técnicas. Por lo tanto, cualquier dispositivo con servicios como el acceso a Internet puede verse afectado por estas acciones maliciosas, debido a que no responden a una motivación única.

Figura 30: Intereses detrás de los delitos cibernéticos.
Fuente: Pixabay (2020), adaptado por labSEAD-UFSC (2020).

Como consecuencia, se estableció un contexto en el que a todo momento surgen nuevas prácticas ilícitas, y a una velocidad acorde con el surgimiento de nuevas tecnologías. Cuando se lanzan nuevas aplicaciones y son introducidas al mercado, los delincuentes analizan sus vulnerabilidades hasta encontrar la mejor manera de utilizarlas como medio de prácticas delictivas.

Figura 31: Las aplicaciones suelen ser objeto de delitos. **Fuente:** Pixabay (2020).

Las aplicaciones son sistemas, y el funcionamiento de estos deriva de la manipulación del usuario, muchas veces no imaginamos que estamos ejecutando un código al hacer un "clic". Debido a la falta de conocimiento, sobre todo, respecto a rutinas de seguridad, las personas son fácilmente victimizadas por:

- Ingeniería social — convencimiento de proporcionar una contraseña.
- Intrusión – deshabilitar los factores de protección.

Todos estos comportamientos demuestran vulnerabilidades que los creadores de estos procesos, no tenían previsto, pues no se percataron que carecían de una protección sistémica mediata.

Figura 32: Seguridad de los sistemas. **Fuente:** Pixabay (2020).

Sin embargo, la solución al problema presentado anteriormente no depende únicamente de incorporar nuevas estrategias corporativas para mayor seguridad, sino también, de aplicar **nuevas formas de control y criminalización de estas conductas perjudiciales**.

El impacto sobre el Estado en este contexto es grande, cada vez se hace más necesario adoptar políticas públicas criminales orientadas a prevenir y reprimir este fenómeno a fin de reducir de manera efectiva los delitos cibernéticos.

Figura 33: El delito cibernético se ha convertido en un problema para el Estado. **Fuente:** Pixabay (2020), adaptado por labSEAD-UFSC (2020).

En general, incluso si se tratan de delitos comunes, es decir, aquellas conductas antijurídicas que se pueden practicar fuera del ciberespacio, el *modus operandi* aplicado en estos delitos está compuesto por elementos peculiares que permean en la comprensión ontológica de este tipo de criminalidad.

Los delitos cibernéticos tienen características peculiares, capaces de hacer ver este tipo de delito como uno difícil de reprimir.

Figura 34: Delitos cibernéticos y sus características. **Fuente:** labSEAD-UFSC (2020).

Veamos, a continuación las especificaciones de cada una de esas características.

Virtualidad

Se trata de los casos en cuáles las acciones son llevadas a cabo en el entorno cibernético, los elementos conductuales, los agentes y el bien legal violado; son inmateriales. Entendemos, entonces, que prevalecerán dos premisas:

Figura 35: Supuestos del entorno o ambiente cibernético. **Fuente:** labSEAD-UFSC (2020).

Por lo tanto, debemos considerar la dificultad de adaptar estos hechos a los delitos tradicionales, pues algunos de ellos requieren la presencia de elementos normativos que suelen ser incompatibles con la realidad del entorno cibernético. Por ejemplo:

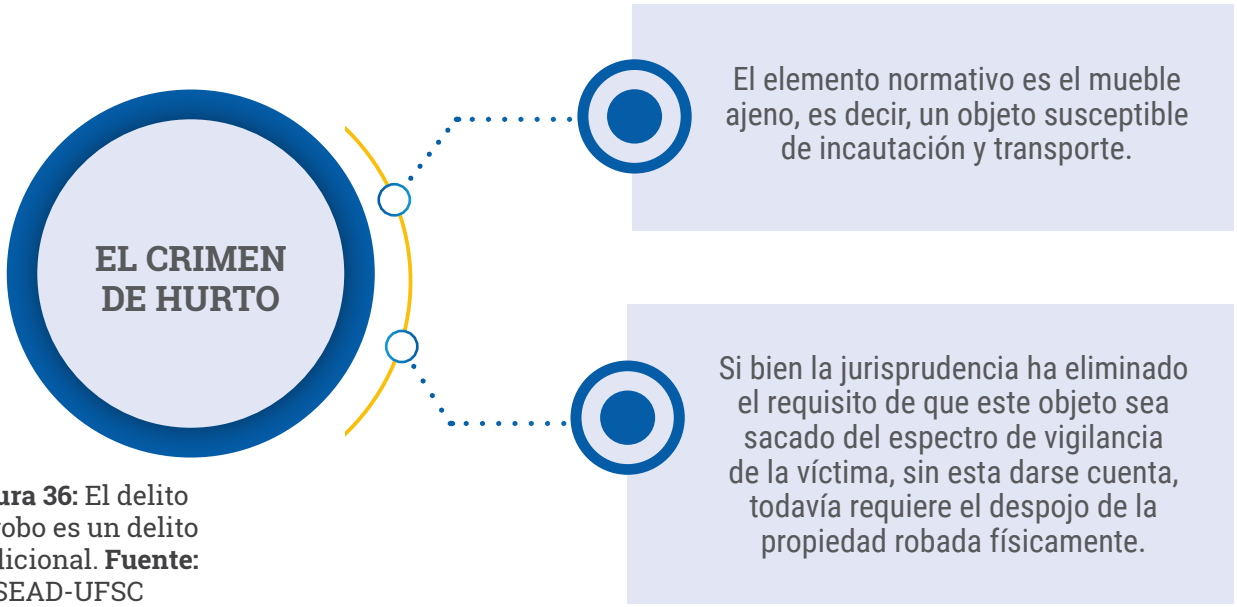


Figura 36: El delito de robo es un delito tradicional. **Fuente:** labSEAD-UFSC (2020).

Al tratarse de datos sustraídos, el elemento normativo no es físico, lo que puede dar lugar a discusiones sobre la naturaleza típica de la conducta. De la virtualidad derivan dos características, como el anonimato de los agentes y la transnacionalidad, es decir, la escena del crimen.

¡Compruébalo!

Anonimato

Los delincuentes son los que realizan acciones maliciosas anteriormente descritas, pero siempre están representados por entidades virtuales, utilizando un *nickname*, por ejemplo. En una dimensión donde todas las personas involucradas interactúan a través de cuentas y perfiles, **la acción directa de manos humanas no sucede taxativamente**.

Figura 37: En el ciberespacio podemos tener varios perfiles. **Fuente:** Pixabay (2020).

Siempre habrá una interfaz entre el mundo real y el digital. Este enlace constituye sólo una capa que separa a la persona del ciberespacio.

> Entre el usuario y su proveedor de conexión, existe un dispositivo. Entre ese proveedor de conexión y el proveedor responsable de administrar la aplicación a la cual accede este usuario, hay aún más intermediarios, y así sucesivamente.

En la dimensión virtualizada, la accesibilidad a ciertos ambientes artificiales puede suceder a través de varios factores interconectados.

En cada uno de ellos, el agente puede usar esos otros medios, para anonimizar a sí mismo. El uso de máquinas virtualizadas y VPN, acrónimo de *virtual private network*, son ejemplos de cómo es posible ese enmascaramiento.

Transnacionalidad

Este aspecto está relacionado con la conducta, puesto que los actos de ejecución pudieron tener lugar en un país determinado, pero los resultados de esa acción, pueden

terminar impactando en el mundo real y perjudicar a personas ubicadas en territorio extranjero.

Figura 38: Un delito puede ocurrir en cualquier parte del mundo y afectar a un país determinado.
Fuente: Freepik (2020).

En esta condición, los temas relacionados con la escena del crimen y la jurisdicción para el procesamiento penal terminan llegando a los tribunales. Algunas de estas controversias aún no han sido resueltas por los tribunales superiores de Brasil.

Dinamismo

Otra característica de los delitos cibernéticos está relacionada con las permanentes innovaciones tecnológicas, generalmente éstas se desarrollan más rápido que la implementación de soluciones normativas. Eso es una realidad mundial.

Figura 39: Bigdata.
Fuente: Pixabay (2020).

Incluso en países considerados hiper-estructurados en relación con su protección cibernética, como Estados Unidos, también existe una gran preocupación por el poder invasivo de las nuevas tecnologías, especialmente con la llegada del Internet de las Cosas, *Internet of Things* (IoTs).

Estos microdispositivos traen consigo sensores y sistemas integrados, previamente programados para recopilar la mayor cantidad datos, que serán estudiados con inteligencia artificial.

> Sin embargo, existe un gran riesgo de que gobiernos extranjeros accedan a esta información y la utilicen en la llamada **guerra cibernética**, una vez que hayan descubierto cómo aprovechar la fragilidad de los sistemas de una nación.

Como resultado, tres aspectos han llevado a la creciente necesidad de cooperación entre las fuerzas de seguridad del Estado y el sector privado en relación con el procesamiento de datos de que navegan entre proveedores, servidores y empresas de hospedaje web:

- Es innegable la magnitud de los posibles daños consecuentes de aquellos delitos que alcancen repercusiones internacionales e incluso globales.
- La facilidad de comprometer las infraestructuras críticas de estos países.
- La baja resiliencia y el limitado poder de respuesta, tanto de estas estructuras gubernamentales como de estructuras particulares ante los posibles ataques cibernéticos de un país.

Especialidad técnica

En el caso de delitos cibernéticos específicos, los delincuentes demuestran elevados conocimientos técnicos requeridos para su ejecución. Incluso para perpetrar algunos delitos ya

comunes en el ciberespacio, cómo mínimo, el delincuente debe hacer vida activa en el ciberespacio.

Figura 40: *Hackers* también pueden ser llamados ciberdelincuentes. **Fuente:** Pixabay (2020).

Si bien se estableció la llamada Era de la Información, aún existe cierto número de personas sin acceso al mundo digital, lo que imposibilita su práctica. Para que un individuo pueda publicar un comentario difamatorio en una red social, lógicamente será necesario que esté suscrito y conectado a ella.

Cabe mencionar que en casos de delitos más especializados, como los delitos financieros arquitectos tecnológicamente, las organizaciones de ciberdelincuentes funcionan como empresas y cuentan con miembros especializados para cada tipo de trabajo y ocupación.

Una organización de esa naturaleza puede contener la estructura de una organización empresarial, con la diferencia de que estos ciberdelincuentes trabajan sin horarios fijos, días festivos y/o fines de semana. Por lo general, se organizan de la siguiente manera:

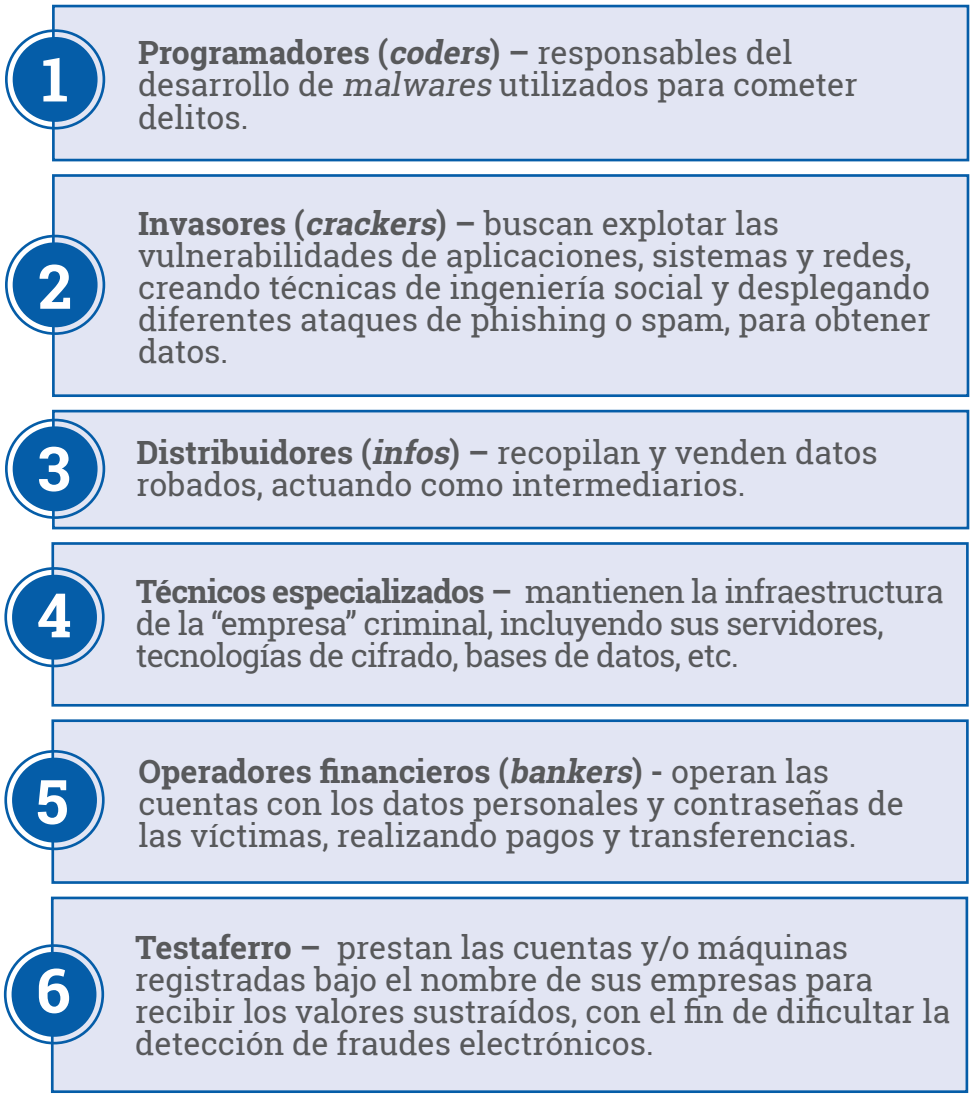


Figura 41: Funcionamiento de las organizaciones deciberdelincuentes. **Fuente:** labSEAD-UFSC (2020).

Los líderes de cada organización pueden ocupar las funciones de los personajes anteriores o, personas sin conocimientos técnicos, pero ejercen la labor de seleccionar los equipos y definir sus objetivos.

Clase 5 – Principales Modalidades de Delitos Cibernéticos

CONTEXTUALIZANDO...

En esta clase, comprenderemos cómo se configuran algunas de las principales modalidades del delito o crimen cibernético dentro de la legislación y cómo estos delitos difieren de los crímenes tradicionales.

CRÍMENES Y LEGISLACIÓN

En el caso de un entorno exclusivamente virtualizado, cuyas dimensiones son inmensurables y esencialmente dinámicas, aparecen continuamente nuevas modalidades delictivas.

Por lo tanto, corresponde a los gobiernos de los países establecer políticas públicas para la prevención y represión de estos actos ilícitos. Por ello, se considera que la característica del tecnicismo, presente en estos casos, requiere de un instrumento cada vez más técnico, que esté capacitado y en condiciones de mantenerse actualizado en relación con las acciones ofensivas que se crean y propagan en la Web.

Figura 42: Aumento de la seguridad cibernética por parte de los gobiernos. **Fuente:** Freepik (2020).

Ya se admite la existencia de un mercado centrado en el ciberdelito, considerándose como principales características de su supervivencia:

- Ambiente propicio gracias al anonimato.
- Bajo costo y riesgo operativo.
- Gran rentabilidad económica.

No es el objetivo de este contenido establecer un listado taxativo sobre los delitos cibernéticos, pero vamos a catalogar los comportamientos más conocidos en el mundo virtual, especialmente aquellos que el legislador ya definió **como un tipo específico**, habilitando su criminalización.

Delitos cibernéticos más conocidos

Invasión de dispositivos informáticos y desarrollo e intercambio de información *malware*.

El concepto legal de invasión de dispositivos informáticos como delito, se encuentra tipificado Código Penal Brasileño de la siguiente manera:

> *Invadir el dispositivo informático de otra persona, conectado o no a la red informática, mediante la violación indebida de un mecanismo de seguridad y con el propósito de obtener, manipular o destruir datos o información sin autorización expresa o titular del dispositivo o instalar vulnerabilidades para obtener una ventaja ilegal. (caput del Art. 154-A del Código Penal Brasileño, traducción nuestra).*

El primer párrafo del citado artículo establece que incurre en este delito:

> *Quien produzca, ofrezca, distribuya, venda o difunda un dispositivo o programa informático con el fin de permitir la práctica de la conducta definida en el caput. (caput del Art. 154-A del Código Penal Brasileño, traducción nuestra).*

Art. 266 del Código Penal, en su párrafo primero, establece **la interrupción o alteración de los servicios informáticos o telemáticos de utilidad pública**, como delito cibernético, describiendo también las acciones para detener o dificultar la restauración de estos servicios.

Cuando esto ocurre a través del entorno virtual, la mayoría de las veces es a través del ataque a la disponibilidad de los sistemas, realizado por la acción conocida como DoS (Denial of Service).

La denegación de servicios es el objetivo de este ataque, este apunta a generar una sobrecarga, lo que impide el acceso a otros usuarios. En su modalidad distribuida (DDoS), es generalmente realizada en redes Botnet, que atacan por obediencia a un comando remoto.

También tenemos algunos delitos específicos en cada categoría. ¡Conócelos!

Delitos contra el honor por medios electrónicos

Antes de la llegada del artículo mencionado, la divulgación de imágenes íntimas se tipificaba como un delito cibernético común.

La especialización, por voluntad de la legislación, destacó esta categoría que incluye aquellas conductas que lesionan el “honor” legal de la víctima, cuando el autor utiliza los medio tecnológicos para materializar su ilícito.

Figura 43: Crímenes contra el honor.
Fuente: Pixabay (2020).

Ahora bien, **la exhibición masiva de la escena de una violación y/o violación de personas vulnerables, cualquier escena sexual o pornográfica**, por medio de Internet, está tipificada en el Art. 218-C del Código Penal Brasileño.

> Aplicable a cualquier propagación de la conducta antes mencionada, así como desnudez o escenas de sexo no consentidas por la víctima.

En este caso concreto, es destacable el avance legislativo en la sanción de la llamada **venganza digital o pornográfica**, que todavía es altamente reportado en las comisarías, especialmente cuando las relaciones sentimentales, terminan.

La Ley **11.829 / 2008** (puedes profundizar en este *link* http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm) caracterizó el abuso de niños y adolescentes a través de Internet como un delito cibernético al Estatuto de la Niñez y la Adolescencia (ECA).

Figura 44: Compartir archivos con imágenes de pedofilia es un delito. **Fuente:** Pixabay (2020).

Se tipificó también el almacenamiento e intercambio (venta, cesión, difusión, etc.) de archivos digitales que contengan escenas sexuales o que representen desnudos de niños y adolescentes.

Crímenes de odio, disculpas y discriminación étnica-racial en Internet

Estos delitos son cada vez más populares en el país, donde muchas personas confunden el ejercicio de derechos consagrados constitucionalmente, como la libertad de expresión y la expresión de pensamiento, con acciones ilícitas. Se trata de crímenes contra los derechos supraindividuales.

En Brasil sigue habiendo escasez de legislación sobre este tipo de delitos, sobre todo, cuando se cometen en el ambiente cibernético.

Hurto mediante fraude por medios electrónicos

Con base en el Código Penal Brasileño, en su §4, II, del Art. 155, es la sustracción de recursos financieros por medios electrónicos, y en el escenario del espacio virtual, generalmente precedido de ataques infligidos para obtener datos personales y credenciales de acceso.

En los casos de ataques contra instituciones financieras, cuyos sistemas están protegidos en gran parte por algoritmos encriptados, los delincuentes utilizan técnicas de ingeniería social, como *phishings*, páginas falsas con formularios para completar datos sensibles de acceso; y *keyloggers*, fotocopiadoras de caracteres escritos, para obtener la información necesaria para acceder a las cuentas de las víctimas.

Fraude electrónico

De la misma manera que en los delitos mencionados, los ciberdelincuentes utilizan y abusan de la ingeniería social para engañar a las personas y obtener ventajas indebidas.

Un ejemplo clásico son los sitios web de subastas en línea que diariamente llevan a cientos de personas a enviar grandes sumas de dinero a organizaciones criminales, creyendo que están pagando la "oferta" señalada para la adquisición de algún bien.

Figura 45: Nuevas formas de cometer delitos. **Fuente:** Pixabay (2020).

Realmente, este sitio web cuenta con elementos gráficos que convencen a las víctimas de su supuesta legitimidad, y estas, atraídas por los bajos valores que ofrece, terminan cediendo los valores señalados, generalmente para las cuentas de "testaferros" que forman parte de los grupos delictivos.

Extorsión cibernética

Esta modalidad delictiva es muy común en Brasil y puede configurarse de diferentes formas. De la forma más sencilla, podemos mencionar los casos en los que el delincuente y el extorsionado mantienen algún tipo de contacto a través del ciberespacio, y el primero, obtiene imágenes íntimas en archivos para exigirle valores económicos a cambio de no propagar esa información, o se compromete a destruirla, una vez que el pago sea efectivo.

Figura 46: Crímenes de extorsión cibernética. **Fuente:** labSEAD-UFSC (2020).

Cabe destacar que la eliminación definitiva de datos es algo muy difícil de lograr, en cuanto a tecnologías de la información, considerando las múltiples técnicas de copia, taquigrafía y recuperación de activos digitales. La forma más sofisticada que se encuentra en la actualidad es el *ransomware*. Es un tipo de *software* dañino, que restringe el acceso al sistema infectado con una especie de bloqueo y cobra un rescate en criptomonedas para que se pueda restaurar el acceso.

Solo mencionamos los delitos cometidos en el ciberespacio que se consideran más recurrentes en la actualidad.

> No se excluyen otras prácticas posibles en la dimensión virtual, como, por el ejemplo, el ataque perpetrado por un dron que es operado por manos humanas, el cual podría resultar en la muerte de una persona en el mundo físico.

Los delitos con menor potencial o los delitos menores también son muy comunes en Internet, tales como la perturbación de la tranquilidad a través de mensajes electrónicos, por ejemplo.

En las próximas clases, vas a tener acceso a un enfoque descriptivo sobre las principales modalidades criminales perpetradas en el ciberespacio, con énfasis en el tratamiento legal proporcionado por el legislador brasileño y la Convención de Budapest sobre el Delito Cibernético.

Referencias

BRASIL. [Constituição de 1988]. **Constituição da República Federativa do Brasil**. Brasília: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 31 jul. 2020.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jul. 2020.

COLLI, M. **Cibercrimes**: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2017.

FLATICON. 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 5 jul. 2020.

FREEPIK. 2020. Disponível em: https://www.freepik.com/. Acesso em: 13 Ago. 2020.

FURLANETO NETO, M.; GUIMARÃES, J. A. C. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: http://daleth.cjf.jus.br/revista/numero20/artigo9.pdf. Acesso em: 30 jan. 2020.

PEXELS. 2020. Disponível em: https://www.pexels.com/pt-br/. Acesso em: 04 jul. 2020.

PIXABAY. 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 04 jul. 2020.

ROSSINI, A. E. de S. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SYDOW, S. T. **Crimes informáticos e suas vítimas**. 2. ed. Saraiva: São Paulo: 2015.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 02 jul. 2020.

VIANNA, T. L. **Fundamentos de direito penal informático**. Rio de Janeiro: Forense, 2003.

MÓDULO 3

VESTIGIOS DIGITALES Y PRESERVACIÓN

Presentación

En este módulo, reflexionaremos sobre algunas situaciones pertinentes acerca de las **investigaciones penales de los delitos cibernéticos**.

¿Qué significa el vestigio, la evidencia y la prueba en el entorno virtual? ¿Es posible que un criminal cibernético deje algún vestigio que pueda contribuir a la investigación?

Por lo tanto, también definiremos la **escena del crimen** en el contexto del ciberespacio, con el fin de comprender cómo se puede definir la jurisdicción responsable del proceso de investigación. Y, por último, analizaremos algunos **procedimientos necesarios para apoyar a la víctima,** a través del registro correcto de la denuncia y las pruebas, que son puntos indispensables para que ocurra una investigación exitosa.

OBJETIVOS DEL MÓDULO

Entender lo que es **vestigio**, **evidencia** y **prueba** en el contexto del crimen virtual, definir la **escena del crimen** en el contexto del ciberespacio, entender cómo se define la jurisdicción en estos tipos de delitos, así como analizar los procedimientos necesarios para recopilar información relevante para el proceso de investigación de los delitos cibernéticos. Además, comprenderemos la necesidad de registrar los vestigios y la importancia de proporcionar apoyo a la víctima.

ESTRUCTURA DEL MÓDULO

- **Clase 1 –** Vestigios, Evidencias y Pruebas en el Entorno Cibernético.
- **Clase 2 –** Escena del Delito Cibernético y Cadena de Custodia.
- **Clase 3 –** Preservación de Vestigios Digitales a través de *Internet*.
- **Clase 4 –** Otros Medios de Preservación de la Evidencia Digital.
- **Clase 5 –** Recopilación de Información Adicional y Entrevista Especializada.

Clase 1 – Vestigios, Evidencias y Pruebas en el Entorno Cibernético

CONTEXTUALIZANDO...

En la investigación criminal, siempre tenemos el vestigio, la evidencia y la prueba. ¿Y cómo es en el entorno virtual?

En esta clase, comprenderemos cómo ocurre el principio de intercambio en el contexto de los delitos cibernéticos y cómo se puede buscar vestigios que contribuyan al éxito del proceso de investigación.

EL CRECIMIENTO DE LOS DELITOS CIBERNÉTICOS

La delincuencia en el entorno cibernético se expande de forma exponencial en todo el mundo, lo que revela la fragilidad de los Estados en la aplicación de medidas de prevención y combate.

> Cada día, las empresas de seguridad especializadas en detección de intrusiones reportan millones de ataques en contra de sistemas corporativos y dispositivos domésticos. Al mismo tiempo, se sabe que sólo una pequeña fracción de estos actos ilícitos se denuncian a la policía, para luego ser procesados y juzgados.

Esto se justifica por las características de estos delitos, que suelen ser de naturaleza **virtual**, **transnacional** y **especializada**.

Se trata de conductas que pueden llevarse a cabo a distancia, al utilizar diferentes métodos para ocultar las direcciones de conexión, así como cualquier otro elemento intangible que pueda promover la rastreabilidad por parte de los órganos policiales competentes.

Figura 1: La conexión puede ocurrir en cualquier parte del mundo. **Fuente:** labSEAD-UFSC (2020).

Ciertamente, el mayor desafío en este ámbito es la producción de pruebas. Algunos ataques dejan pocos vestigios que puedan ser utilizados por los investigadores.

Algunos aspectos tienen consecuencias importantes para la identificación del país, empresa o lugar donde se transmite o almacena la evidencia, entre los que podemos mencionar: la descentralización de las fuentes de información y la ausencia de control estatal.

Figura 2: Seguimiento de datos. **Fuente:** Pixabay (2020).

En general, los hallazgos de los delitos cibernéticos no resultan concluyentes debido a estas dificultades vinculadas a la propia naturaleza de la red y a la virtualidad de las pruebas de dichos delitos.

Normalmente, el acceso inmediato a los datos es imprescindible. Dichos datos dependen del servicio de almacenamiento de los proveedores y, en casos más extremos, de la cooperación entre los organismos encargados de hacer cumplir la ley para materializar las pruebas.

La legislación de la mayoría de los países, como es el caso de Brasil, condiciona el suministro de datos a las órdenes judiciales, emitidas sólo después de un cuidadoso análisis de mérito.

> También podemos destacar otra característica de los delitos cibernéticos, como el dinamismo, el cual puede jugar un rol tan importante para la investigación como la virtualidad y la transnacionalidad, como vimos anteriormente.

La virtualización de las rutinas y los modelos de negocio significa que los objetos materiales vinculados a los delitos tradicionales también están cada vez más restringidos a los formatos electrónicos.

En la actualidad, también es perfectamente permisible que, en los actos preparatorios para la ejecución de delitos comunes, el autor tome alguna medida en el entorno cibernético y deje constancia sobre su paradero o algún diálogo con un involucrado en la escena del crimen. Las investigaciones criminales que no dependen de evidencia digital se están convirtiendo en la excepción.

Figura 3: Las pruebas digitales son diferentes de las pruebas físicas en los procesos de investigación. **Fuente:** Pixabay (2020).

Debido a la interactividad constante del hombre con este entorno, el flujo de información es intenso, especialmente con la difusión de las plataformas de redes sociales, donde se genera una gran cantidad de datos.

Figura 4: Flujo internacional de uso de la red de Internet. **Fuente:** Freepik (2020).

Las bases de datos y los repositorios se alimentan en todo momento, en la misma proporción que se pueden eliminar, modificar y sobrescribir. Estos aspectos refuerzan la idea de que las pruebas producidas en este medio son extremadamente "perecederas", es decir, pueden desaparecer fácilmente.

> En este sentido, es importante preservar los datos de los sistemas de computadoras o dispositivos de almacenamiento para la efectividad de un futuro caso penal.

En 1892, el Dr. Edmond Locard publicó una obra considerada un clásico de la criminalística: *La investigación criminal y los métodos científicos*.

¡A continuación veremos cómo el estudio de Locard revolucionó la investigación criminal!

EL PRINCIPIO DEL INTERCAMBIO DE LOCARD

En las primeras páginas, Locard (1939) inmortalizó un pensamiento que llegó a ser conocido como el "principio del intercambio de Locard". El científico especuló que cada vez que se hace contacto con otra persona, lugar o cosa, el resultado es un intercambio de materiales físicos.

Locard creía que no importa a dónde vayan los criminales o lo que hagan, al estar en contacto con las cosas, dejan todo tipo de evidencia, entre los que se incluyen el ADN, huellas dactilares, cabello, células de la piel, sangre, fluidos corporales, ropa, fibras y más. Al mismo tiempo, también toman algo de la escena.

El principio del intercambio en el mundo cibernético

Muy cerca de cumplir un año de existencia, el principio todavía parece actual y totalmente aplicable al mundo cibernético, algo inimaginable para Locard en su época.

Figura 5: El principio del intercambio de Locard en el medio digital. **Fuente:** Freepik (2020).

Como hemos visto anteriormente, el acceso y la transferencia de paquetes, en este entorno proporcionado por las redes de comunicación, se deben a la acción de protocolos, especialmente el TCP/IP.

> Por lo tanto, cada operación realizada en un sistema operativo es registrada como un evento.

Toda la operación es registrada a partir de *logs* (eventos), y estos datos se convierten en la principal fuente de información para el investigador para recrear la escena del crimen, así como para contextualizar a los usuarios involucrados en la misma. En resumen, se lleva a cabo un intercambio perfecto, como Locard teorizó.

Figura 6: Toda operación realizada en un sistema operativo es registrada como un evento. **Fuente:** Freepik (2020).

Es importante entender que los materiales físicos —según las palabras del Dr. Locard— dejados en la escena del crimen, así como los eventos computacionales antes mencionados, pueden clasificarse según su estado o etapa en la que se encuentren en la investigación, como: **vestigios**, **evidencia** y **pruebas**.

VESTIGIOS

Vestigio es derivado de la palabra latina *vestigium*, que significa: rastro, pista, prueba o señal.

El Código Procesal Penal Brasileño fue enmendado recientemente por un conjunto de leyes, incluida la Ley 13.964/2019, que incluye el artículo 158-A, el cual conceptualiza al vestigio de la siguiente manera:

> *Todos los objetos o materiales, visibles o latentes, encontrados o recogidos, relacionados con un delito penal. (BRASIL, 2019, traducción nuestra).*

En este sentido, los vestigios son elementos materiales o inmateriales (objeto) encontrados en una escena del crimen que pueden o no relacionarse con ella. Constituyen la materia prima de la producción probatoria, presentada en su estado más sublime.

EVIDENCIAS

Las **evidencias** son vestigios que, luego de ser analizados por los peritos a través de exámenes, se demuestra que están directamente relacionados con el delito investigado.

Se clasifican de esta forma cuando pasan por la fase transitoria.

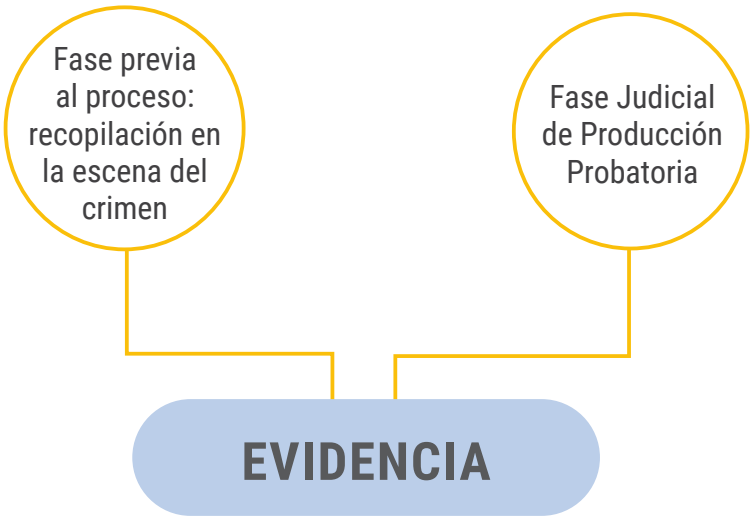


Figura 7: Una evidencia comienza a partir de un vestigio. **Fuente:** labSEAD-UFSC (2020).

Aunque los demás conceptos también están relacionados entre sí, el concepto de evidencia, por estar en este espacio transitorio, es el que demuestra una mayor interconexión con los demás, por lo que se reconoce como evidencia a cualquier material o dato vinculado a un agente o evento provocador. Durante su análisis, es necesario someterse a procesos analíticos de evaluación y clasificación, a fin de extraer varias conclusiones.

Una de las conclusiones esperadas es si el vestigio tiene o no un vínculo con el delito que se está analizando. En el momento en que exista una información que confirme el vínculo del vestigio, este pasa a ser denominado "evidencia".

PRUEBAS

La **prueba** en una etapa del proceso, en la que las evidencias fueron agregadas a los hechos analizados por la autoridad policial (en caso de una investigación) o ministerial (en caso de una denuncia).

La prueba original de una evidencia siempre es el resultado de un procedimiento pericial y, por lo tanto, es objetivo. En el mismo código procesal, el legislador establece, en el artículo 239, la definición de prueba, considerando:

> *[...] la circunstancia conocida y probada, que, en relación con el hecho, autoriza, por inducción, el inferir la existencia de otra u otras circunstancias. (BRASIL, 2019, traducción nuestra).*

A partir de esta definición, entendemos que una prueba puede llevar a otra, en caso de que las circunstancias lo permitan. Debido a que la prueba se basa en una circunstancia conocida y probada y el otro deriva de éste, ambas pruebas no tienen la misma notoriedad.

Por lo tanto, un elemento recogido en la escena del crimen es un vestigio hasta que es analizado por los forenses y se constata su relación con los hechos establecidos, para luego considerarse una evidencia. Este elemento recopilado forma parte de la fase previa al procedimiento, y cuando se agrega al proceso, se convierte en una prueba.

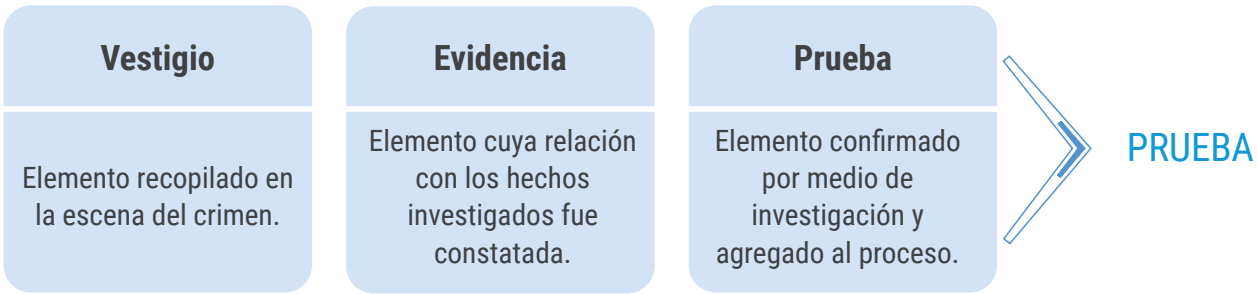


Figura 8: Etapa procesal de la prueba. **Fuente:** labSEAD-UFSC (2020).

La primera prueba, por ser una circunstancia conocida y probada, suele presentarse como una prueba objetiva, mientras que la siguiente se presenta como una prueba sujeta a interpretación, a veces objetiva o subjetiva. Un concepto distinto es la prueba indiciaria, que es cuando la prueba resulta de la subjetividad, es decir, de la interpretación.

VESTIGIO CIBERNÉTICO

En el entorno cibernético, se admite la existencia de vestigios digitales, que encajan perfectamente en esta distinción teórica, y que abarca signos, marcas u objetos dejados por los usuarios en el entorno virtual.

Actualmente, es muy difícil encontrar situaciones en las que, directa o indirectamente, estos insumos tecnológicos no estén involucrados en acciones cotidianas.

Figura 9: Los vestigios cibernéticos pueden ser evidencia electrónica. **Fuente:** Pixabay (2020).

En este contexto, se consideran diversos vestigios que pueden ser empleados como pruebas electrónicas, tales como:

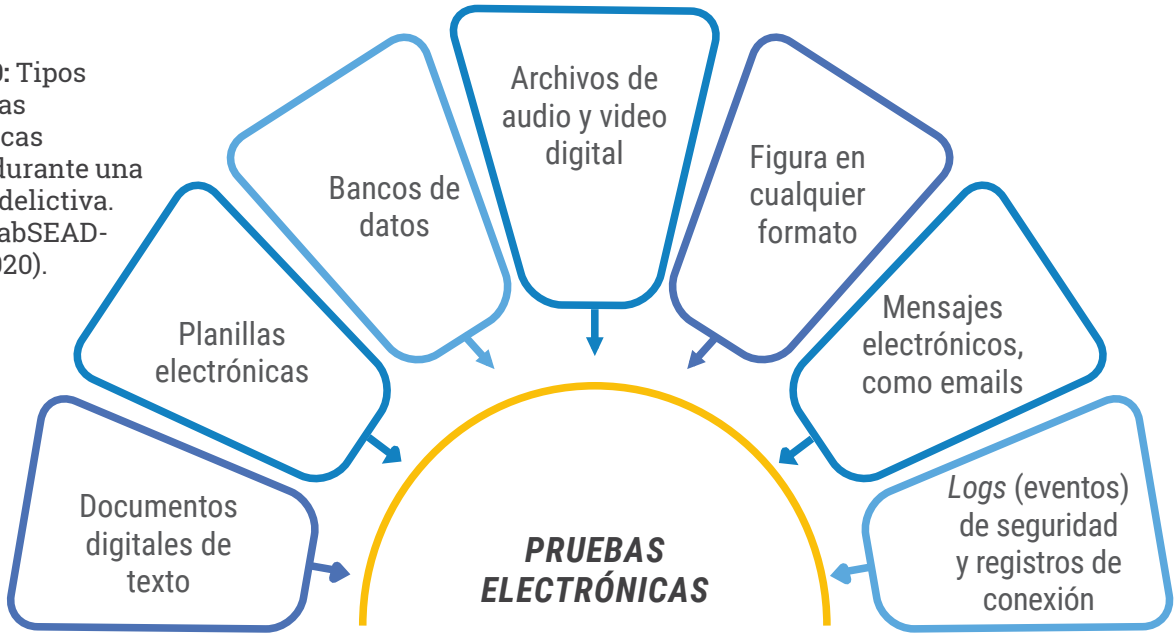


Figura 10: Tipos de pruebas electrónicas dejadas durante una práctica delictiva. **Fuente:** labSEAD-UFSC (2020).

La recopilación de estos vestigios, los cuales fueron dejados durante la práctica delictiva, suele implicar la habilidad o especialización del agente responsable, que puede ser o no un perito oficial.

El uso de los recursos tecnológicos de extracción de datos también contribuye en gran medida a las investigaciones, así como al apoyo de los proveedores de servicios.

> Se denominan vestigios digitales pasivos a aquellos presentados por los proveedores de servicios o extraídos de dispositivos capaces de almacenar datos para su posterior recopilación.

Un ejemplo de vestigio digital son los informes de eventos proporcionados por las operadoras, desde los cuales se puede rastrear la dirección IP del usuario que cometió el delito y deducir cuándo se creó y dónde se originó.

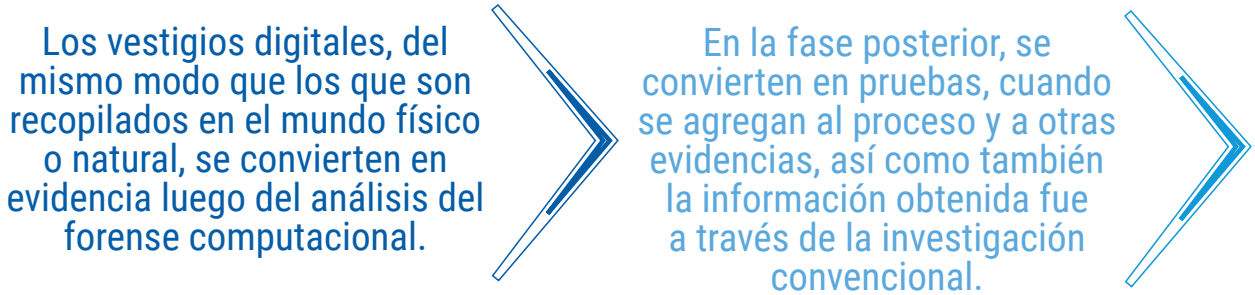


Figura 11: Relación de vestigios, evidencia y pruebas en los delitos cibernéticos. **Fuente:** labSEAD-UFSC (2020).

Estos vestigios podrán analizarse en cualquier momento, siempre que se respeten los plazos procesales y prescriptivos.

> La imposibilidad, es decir, la no recuperación de vestigios pasivos, puede ser jurídica, es decir, la provisión no está autorizada por ley, o técnica, ya sea por datos inaccesibles por criptografía indescifrable o incluso por eliminación de datos.

Los **vestigios digitales activos** sólo pueden recolectarse en el ambiente *online*, cuando el objetivo haya iniciado sesión en un *sitio web* o sistema. Estos datos se extraen en el momento en que el sospechoso realiza una publicación o la edita.
La **producción de esta prueba** está directamente ligada al elemento **oportunidad**, mientras que en el caso de los **vestigios pasivos**, es más importante el **elemento posibilidad**.

Clase 2 – Escena del Delito Cibernético y Cadena de Custodia

CONTEXTUALIZANDO...

¿Cómo definimos la escena del crimen?

Para la definición clásica, la escena del crimen puede entenderse como una zona física en la que se ha cometido un ilícito penal y la que se pueden encontrar vestigios circunstancialmente relacionados, los cuales serán útiles para responder las preguntas más importantes sobre lo ocurrido.

En esta clase, analizaremos cómo se enmarca la idea de escena del crimen en el contexto de los delitos cibernéticos, al considerar las principales indagaciones que rodean el tema: **la autoría**, **la dinámica** y **la materialidad** de este tipo de crimen.

ESCENA DEL CRIMEN

¿Conoces cuál es la base de las ciencias forenses para el inicio de una investigación criminal?

Típicamente, se emplea el Método Quintiliano o 5W2H, del romano Marcus Fabius Quintilianus (c. 35 - c. 100 d.C.). A continuación, observa cómo funciona el 5W2H.

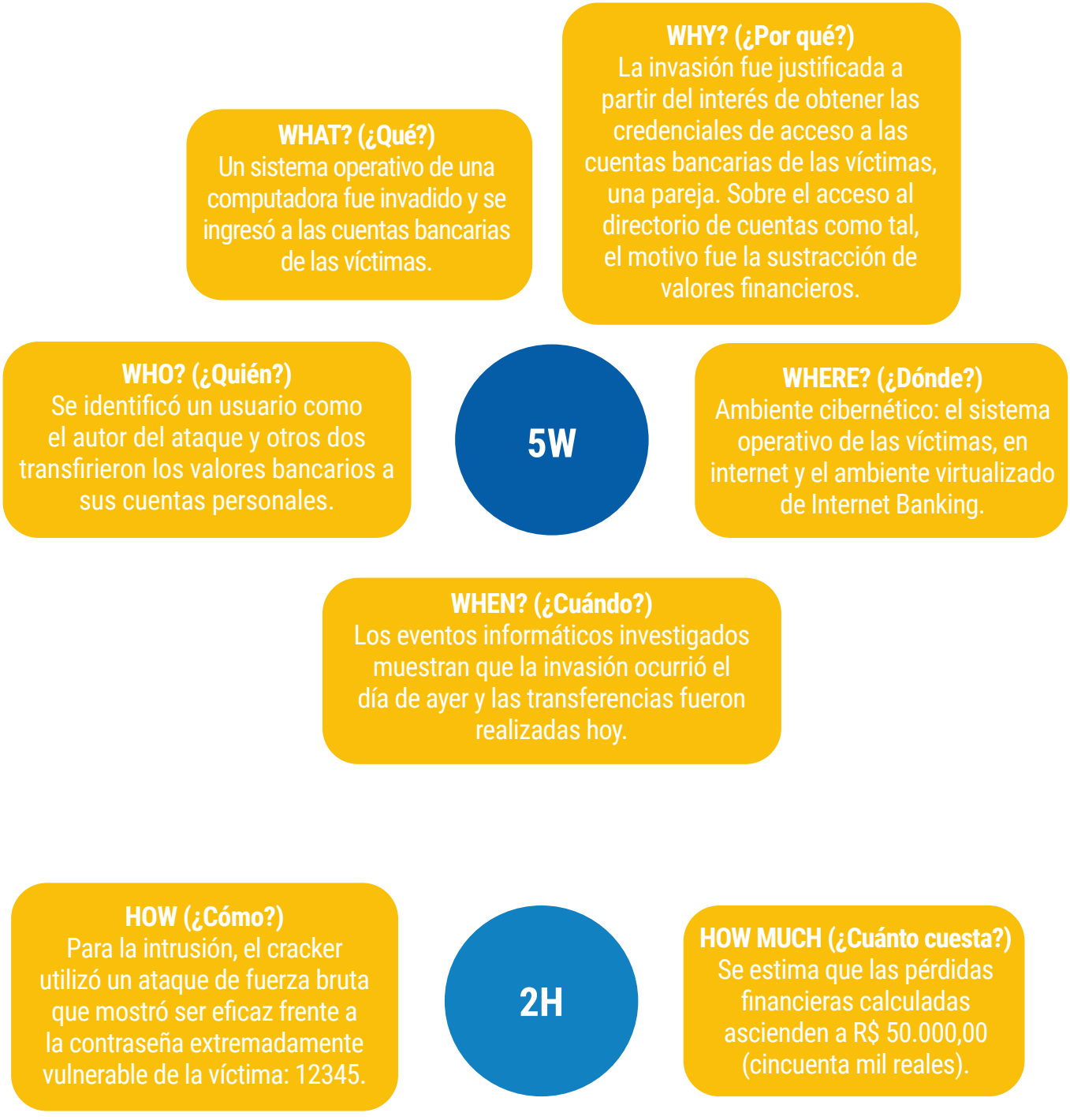


Figura 12: El 5W2H en el contexto de los delitos informáticos. **Fuente:** labSEAD-UFSC (2020).

Las respuestas a estas siete preguntas ciertamente corresponden a la aclaración de un hecho.

La conclusión obvia de que el lugar donde se produce el delito cibernético es el entorno del delito cibernético, es decir, una dimensión virtualizada por naturaleza, tiene consecuencias tanto para la criminalística como para el ordenamiento jurídico.

Escena del crimen cibernético: jurisdicción para el enjuiciamiento penal

Cuando hablamos de Derecho Procesal, observamos que su concepción espacial no es compatible con los criterios que tradicionalmente definen la competencia y jurisdicción para su enjuiciamiento.

El Código Procesal Penal Brasileño, en su artículo 69, determina la jurisdicción a partir de los siguientes criterios.

Figura 13: Requisitos para definir la jurisdicción de un crimen. **Fuente:** labSEAD-UFSC (2020).

¿Cómo emplear la competencia jurisdiccional en el ambiente digital? Después de todo, **no existen dimensiones geográficas ni espacios definibles, y los agentes involucrados están representados por entidades virtuales**, por lo que no ejercen funciones.

Estos aspectos, en principio, pierden sus características reales cuando los actores involucrados se conectan en el ciberespacio. Es necesario personificar una entidad virtual para considerar su prerrogativa debido a la función.

En la Práctica

Un delito cibernético fue cometido por un alcalde de un municipio brasileño. Se identificó el perfil que realizó una publicación. En este caso, con el propósito de establecer la jurisdicción, ¿en qué momento podríamos considerar el cargo del alcalde?

En este caso, el cargo sólo se considerará cuando se haya demostrado el acceso efectivo a la cuenta por el alcalde en el momento del crimen. El artículo 70 del Código de Procesal Penal define la escena del crimen de la siguiente manera:

> *La competencia será, por regla, determinada por el lugar donde se consumió la infracción, o en caso de un intento, en el lugar donde se realizó el último acto de ejecución. (BRASIL, 2019, traducción nuestra).*

El lugar considerado es el **espacio físico** donde se materializaron los efectos del delito o, en la hipótesis de intento, donde se encuentra el agente que ejecutó el último acto del crimen.

Los delitos cibernéticos generalmente se consumen en el propio ciberespacio, como es el caso de los delitos contra el honor, delitos contra la propiedad, entre otros.

Es por ello que la doctrina especializada en los delitos cibernéticos, que se ha establecido en las últimas décadas, ha pedido un cambio de paradigma y el abandono de los conceptos tradicionales para el establecimiento de competencias, establecidas sobre la base de la soberanía territorial.

En cuanto al ejecutor, un ataque de denegación de servicio vía ***botnet*** puede contar con la solicitud de acceso de máquinas, simultáneamente, conectadas desde todos los continentes del planeta.

Una botnet es un número de dispositivos conectados a Internet, cada uno ejecutando uno o más bots. Las redes de bots pueden usarse para realizar ataques DDoS, robar datos, enviar spam y permitir el acceso del atacante al dispositivo y su conexión.

En este contexto, se han detectado varios problemas para la justicia penal en la lucha contra el delito cibernético, especialmente en lo que respecta a la legislación aplicable y la jurisdicción de aplicación.

El primer desafío consiste en localizar datos para definir la ley aplicable.

Localización de datos

Las tecnologías actuales no contribuyen en este aspecto.

En la Práctica

Imaginemos cómo ocurre la computación en la nube: un proveedor de servicios *cloud* (nube) puede tener su sede central en una jurisdicción y aplicar el régimen jurídico de una segunda jurisdicción, mientras los datos se almacenan en una tercera jurisdicción. Los datos pueden reflejarse en otras jurisdicciones o moverse entre las mismas. **¿Cómo podemos entender qué jurisdicción es responsable del crimen?**

El problema central radica en el hecho de que, aunque el ciberespacio es una dimensión virtual y se desarrolla a través de un proceso de inteligencia colectiva, se erige artificialmente sobre pilares físicos. Es decir, su existencia depende de una infraestructura construida y gestionada en el mundo natural.

Figura 14: Los servicios de red son la dimensión física del ciberespacio. **Fuente:** Pixabay (2020).

En este sentido, debemos recordar aquí que la prestación de servicios de red, el ISP, es distribuida en todo el planeta.

> En términos prácticos, la comunicación entre brasileños a través de una aplicación de mensajería involucra proveedores de varios países, además de Brasil.

Por lo tanto, podemos admitir que un acceso único a la red de Internet puede generar vestigios e involucrar a personas que residen en un gran número de jurisdicciones diferentes. Por lo general, surgen dos grandes problemáticas.

1. Sobre la efectiva responsabilidad de determinado país por determinado crimen.
2. Sobre la competencia del poder de la policía para eliminar eventuales problemas.

Figura 15: Problemas para definir la jurisdicción de los delitos cibernéticos. **Fuente:** labSEAD-UFSC (2020).

Los tribunales brasileños han buscado criterios para definir la competencia, mientras reconocen la imposibilidad de definir lugares en el ciberespacio.

Estudio de Caso

En el juicio de 2004 del caso CC 40.569-SP, el Ministro Relator José Arnaldo da Fonseca detalló los hechos y entendió que "las víctimas estaban limitadas por amenazas a través de mensajes electrónicos enviados en Internet, según los cuales se tenía la intención de infligirles un daño injusto si no proporcionaban valores, lo que llevó a las víctimas a ofrecer las noticias del crimen al Ministerio Público. Por lo tanto, no hay manera de entender que existe un mero intento punible, porque el delito se consumó en el lugar donde el afectado recibió los correos electrónicos y a través de éstos tuvo conocimiento de donde se establece la competencia, por lo que el lugar de donde se enviaron los mensajes quedaría sin influencia". (BRASIL, 2004, traducción nuestra).

La Corte Superior de Justicia, en 2018, publicó una encuesta sobre precedentes que juzgaron delitos cibernéticos en Brasil, los cuales interpretaron las normas infraconstitucionales en relación con las prácticas ilícitas cometidas en la red.

Un debate frecuente en los casos que llegan a los tribunales, por ejemplo, se refiere a la competencia de la sentencia con respecto al análisis de los casos en los que el robo tiene lugar a través de la red informática mundial. **El Tribunal Supremo de Justicia brasileño definió la competencia a partir del lugar donde se sustrajo la propiedad de la víctima.**

Saber más

¿Qué pasa con las hipótesis de amenazas hechas por las redes sociales?

En los casos de amenazas hechas por Facebook y aplicaciones como WhatsApp, el mismo Tribunal Superior ha dictaminado que **la sentencia competente para la aplicación de medidas de protección será aquella donde la víctima haya tenido conocimiento de la intimidación**, porque éste es el lugar de consumación del delito previsto en el artículo 147 del Código Penal.

Incluso de esta manera, el lugar del crimen cibernético no sólo es de interés para la aplicación de la ley con fines jurisdiccionales. Sino también lo es para aquellos encargados de recoger vestigios presentes en la escena del crimen, en cuyo caso el comprender sus peculiaridades es fundamental.

En este sentido, no es posible entender que el ciberespacio es un entorno de red. Por lo general, la investigación penal en esta área requiere información de los suscriptores del servicio, incluidos los datos personales de estos contratantes, tales como:

Figura 16: Tipos de vestigios pasivos.
Fuente: labSEAD-UFSC (2020).

Estos vestigios, clasificados como **pasivos,** no pueden ser recopilados en el lugar del crimen, ya que sólo los proveedores tienen estos datos.

> Incluso las direcciones IP, hoy en día, apenas son capturadas *online*, ya que las empresas responsables de las aplicaciones ocultan la IP real u original utilizada por el usuario, por razones de seguridad e infraestructura.

Los datos de contenido que se comparte en la red son de enorme valor para la investigación y, en caso de que exista una oportunidad, deben ser recopilados. Esta declaración se basa en la dificultad de obtener esta información de los proveedores, incluso si está respaldada por una orden judicial.

Figura 17: La protección del suministro de datos dificulta algunos procesos de investigación. **Fuente:** Freepik (2020), adaptado por labSEAD-UFSC (2020).

En algunos países, como los Estados Unidos, existen leyes que prohíben proveer datos extraídos de comunicaciones (Stored Communications Act). Recientemente, se convirtió en una práctica común la recopilación depredadora de datos personales por parte de grandes empresas del sector tecnológico, como Google, Facebook y Amazon, por ejemplo, cuyo modelo de negocios es la monetización de dichas informaciones.

Ante esta realidad, los países han buscado formas de proteger a sus ciudadanos de esta intrusión en su intimidad. La Unión Europea ha promulgado su marco regulador, el RGPD, acrónimo del Reglamento General de Protección de Datos, que entró en vigor en mayo de 2018.

Figura 18: Privacidad del usuario. **Fuente:** Freepik (2020).

Desde entonces, la preocupación por la privacidad de los usuarios se ha convertido en uno de los principales fundamentos del nuevo régimen jurídico creado por esta norma. Esto, de hecho, tuvo repercusiones en la posición de los proveedores de servicios europeos, que comenzaron a restringir el suministro de datos en casos de delitos cibernéticos, incluso cuando lo solicitaban las autoridades.

Los países considerados socios económicos de las empresas europeas también necesitaron adaptarse a esta nueva realidad y modificaron sus leyes protectoras sobre la privacidad digital, basadas en el Reglamento General de Protección de Datos (RGPD). En la práctica, los efectos ya se sienten y la recopilación de datos de fuentes abiertas en Internet se ha vuelto escasa.

Figura 19: Solicitudes administrativas de violación de la confidencialidad y acceso a la información. **Fuente:** Pixabay (2020), adaptado por labSEAD-UFSC (2020).

En cuanto a las solicitudes administrativas y judiciales, los datos que se reciben con mayor frecuencia de los proveedores son la información de los suscriptores, ya que son menos sensibles para la privacidad que el tráfico de datos de contenido.

Por otro lado, otros métodos pueden garantizar que se rastreen los puntos de acceso a la red y que la investigación llegue a una terminal conectada al entorno donde se produjo el delito.

Saber más

La Ley 13.709 del 14 de agosto de 2018, es la Ley General de Protección de Datos Personales, y puedes saber más sobre ella al hacer clic en el *link* a continuación para acceder a la ley en su totalidad.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Como vimos anteriormente, el ciberespacio existe sólo debido a los dispositivos de enlace y acceso que envían, comparten y reciben señales de comunicación, incluidos los terminales de usuario.

> En este nivel, de características físicas, es donde el "internauta" establece una interfaz con el mundo digital y donde también se almacenan los datos, los cuales conforman la escena o lugar del crimen.

Los ordenadores y dispositivos informáticos generalmente almacenan *logs* (información de eventos) internos y otros datos de gran relevancia para el investigador, tales como: imágenes digitales, *software* malicioso, entre otros. La recopilación de estos vestigios a partir de la incautación de máquinas debe cumplir con los dictámenes legales, bajo pena de nulidad de la prueba.

En 2019, a través del artículo 158-A de la Ley 13.964, el término "**cadena de custodia**" fue regulado para la criminalística de la siguiente forma:

> *[...] el conjunto de todos los procedimientos utilizados para mantener y documentar la historia cronológica del vestigio recolectado en escenas o víctimas de delitos, para rastrear su posesión y manipulación a partir desde su reconocimiento hasta el descarte. (BRASIL, 2019b, traducción nuestra).*

El mismo artículo considera que el inicio de la cadena de detención es el momento de la preservación del lugar del crimen o con procedimientos policiales o forenses en los que se detecta la existencia de vestigios.

En el artículo 158B, la legislación enumera las etapas de la cadena de custodia, lo que hace que el vestigio sea rastreable desde su origen. Compruébalo.

Figura 20: Etapas de la cadena de custodia. **Fuente:** labSEAD-UFSC (2020).

La legislación regula la cadena de custodia para los vestigios de delitos en general.

Estas etapas son perfectamente adaptables a los delitos cibernéticos, si consideramos los insumos digitales.
Para su aplicabilidad, es esencial entender que son elementos inmateriales y extremadamente perecederos.

Reconocimiento

En el paso de reconocimiento, los peritos o investigadores deben evaluar todas las fuentes de información disponibles, incluidas las máquinas virtuales, archivos *log* y los dispositivos externos que se hayan utilizado.

Figura 21: Reconocimiento de un vestigio.
Fuente: Pixabay (2020).

El Hash es un algoritmo criptográficamente sólido y no reversible, que se convierte en algo único de la fuente que se está recopilando y que se puede verificar fácilmente más adelante. Esto ocurre de modo que no haya forma de modificar esta secuencia de caracteres.

Al igual que cuando se toman fotografías y huellas dactilares en una escena física del crimen, los profesionales responsables deben usar imágenes forenses para registrar el sistema afectado y los componentes relacionados.

Aislamiento

La integridad del vestigio digital generalmente está garantizada a través del envío de los archivos a una función ***hash*** unidireccional.

Estudio de Caso

La idea central de una función *hash* es recibir una entrada de cualquier extensión y crear una salida de extensión fija. En la práctica, los archivos o imágenes forenses se envían como entrada y el algoritmo crea una secuencia sintética de letras y números aleatorios "a0680c04c4eb53884be77b4e10677f2b".

Esto se denomina resumen de mensaje, y representa un valor único, como si se tratara de una huella digital de los vestigios físicos. La fecha y la hora del *hash* deben coincidir con la hora de recopilación del vestigio.

Del mismo modo, esto debería ocurrir en el momento del examen por los forenses, donde de nuevo el vestigio se someterá a *hash*. En este caso, el resultado debe ser el mismo, a diferencia de la fecha, que será la misma de ese instante.

Saber más

La captura de memoria volátil (*memory dump* o *dump*) también es un acto obligatorio en delitos en desarrollo en la red.

El *memory dump* es un procedimiento de captura, para una reproducción posterior, de todo lo que está en la memoria en un momento determinado cuando se ejecuta el programa.

La volatilidad es una característica de las memorias primarias, que cargan información antes de ser manejada por los procesadores de las computadoras. Sin embargo, cuando el dispositivo del equipo está apagado, estos datos se eliminan.

En la práctica investigativa, es muy común identificar, entre los datos obtenidos en la captura de memoria volátil, aquellos que prueban que el investigado traficaba datos bancarios en cuentas de terceros e imágenes sexuales que involucran niños y adolescentes. El uso de *malware* y claves criptográficas también se detectan comúnmente en estos procedimientos de recopilación.

Clase 3 – Preservación de Vestigios Digitales a través de *Internet*

CONTEXTUALIZANDO...

En las últimas décadas, el aumento en el número de redes sociales ha sido significativo, especialmente debido a la accesibilidad a estas aplicaciones a través de un teléfono inteligente. Por lo tanto, este poder atractivo no pudo ejercer, en la misma proporción, una conciencia ética por parte de sus usuarios.

En esta clase, profundizaremos en nuestros estudios sobre **delitos digitales**, con un enfoque en la preservación de vestigios. ¡Esperamos que aproveches este contenido!

REDES SOCIALES

Este entorno de agrupación social de amplio espectro, capaz de reunir a personas de todas las nacionalidades, razas, clases y credos, es también el espacio donde la mayoría de los ataques contra la dignidad de un ser humano ocurren a través del medio virtual.

> En Brasil, cada día se cometen millones de delitos contra el honor, que se suman a crímenes de odio, delitos menores, amenazas, entre otros.

Estos actos ilícitos se denuncian en las comisarías de policía de todo el país y, a menudo, sólo se registra el informe policial. Aunque el profesional de la seguridad pública se encargue de describir los hechos detalladamente, una acción es extremadamente importante: la preservación de los vestigios digitales.

Figura 22: El vestigio puede estar en la pantalla de su teléfono móvil. **Fuente:** Pixabay (2020).

Esto se justifica debido a la característica del dinamismo de estos delitos, lo que muestra la rapidez con que la información se difunde y elimina de la red.

Estudio de Caso

Se cometió un acto ilícito mediante una publicación electrónica, pero el autor eliminó el mensaje que infringía la ley poco después. En estos repositorios virtuales abiertos, la información llega rápidamente a muchos usuarios de esa aplicación, lo que ya satisface al criminal. Al darse cuenta de que los efectos perjudiciales para la víctima se materializaron según lo planeado, el criminal comienza a preocuparse por un posible proceso penal y luego elimina la publicación, la modifica o incluso sale de la red.

El derecho de eliminación es un **corolario** del derecho al olvido. Con el desarrollo y la proliferación del Internet, el intercambio de información se ha convertido en una constante y ésta puede ser replicada por cualquier usuario que tenga acceso a ella.

Situación que ocurre de otros: consecuencia; resultado.

A partir de entonces, la información circulará libre y eternamente a través de la red. Por lo tanto, la regla dejó de ser el olvido y se convirtió en el registro de todos los hechos, datos e información, lo que da pie a una sociedad donde se recuerda todo sobre todos.

> En este escenario, rescatamos la discusión sobre el "derecho al olvido", es decir, el derecho de la personalidad que garantiza a los individuos la prerrogativa de que ciertos hechos, datos e información sobre su persona no sean recordados en contra de su voluntad.

El Marco Civil de Internet (Ley 12.965/2014), al disponer sobre los derechos y garantías de los usuarios, ha consagrado el acceso a *internet* como esencial para el ejercicio de la ciudadanía, garantizando, en su artículo 7, numeral X, los derechos:

> *La eliminación definitiva de los datos personales que se hayan ofrecido a determinada aplicación de internet, bajo su solicitud, al término de la relación entre las partes, sin incluir las hipótesis para el mantenimiento obligatorio de registros que están previstas en esta Ley. (Art. 7, numeral X, Ley 12.965) (BRASIL, 2014, traducción nuestra).*

Sin embargo, al destacar la salvedad de las hipótesis de mantenimiento obligatorio de registros, también previstas en el Marco Civil de Internet, la legislación se refiere a las hipótesis de mantenimiento y almacenamiento descritas en los artículos 10, 13 y 15.

> De acuerdo con el artículo 7, la norma es siempre el secreto del flujo de información, y no el suministro de datos, sólo excepcionalmente excluido por autorización judicial o solicitud de los órganos administrativos encargados de hacer cumplir la ley, en las hipótesis en que es posible.

En cualquier caso, la preservación de los datos por parte de los proveedores de aplicaciones, como las redes sociales, es esencial.

Figura 23: Facebook es una de las redes sociales más visitadas del mundo. **Fuente:** Pixabay (2020).

Las empresas responsables de la gestión de las redes más visitadas en el mundo, Facebook, Instagram y WhatsApp, tienen plataformas de *law enforcement*, dedicadas a las autoridades de los países que llevan a cabo investigaciones penales.

Saber más

La empresa Facebook Inc, con sede en Estados Unidos y Brasil, posee la plataforma Facebook Records (www.facebook.com/records). Se trata de una interfaz entre el proveedor y las entidades gubernamentales, desarrollada para recibir solicitudes administrativas y judiciales relacionadas con cuentas de redes sociales Facebook e Instagram.

Cualquier agente estatal que aplique la ley puede registrarse al utilizar su dirección de *email* institucional. Al ingresar al entorno virtual, sólo se debe solicitar la preservación de la cuenta investigada en el propio campo.

> Es necesario introducir la URL (dirección de correo electrónico) de la página que desea conservar. El teléfono o *email*, en caso de que sean presentados, también conservan las cuentas vinculadas a ellos. Este procedimiento evitará que los datos de la cuenta sean eliminados.

Aunque la empresa WhatsApp Inc. pertenece al mismo grupo económico, para las cuentas de sus usuarios se creó una plataforma separada. En ambos casos, los proveedores conservan las cuentas durante un período de 90 (noventa) días, que puede ser prorrogable.

Saber más

Whatsapp Records (www.whatsapp.com/records) tiene los mismos requisitos para registrarse y acceder de la plataforma utilizada para las redes Facebook e Instagram, anteriormente mencionadas. La única diferencia es que la búsqueda de usuarios solo se puede hacer por número de teléfono vinculado a la cuenta.

Otras redes sociales a menudo reciben solicitudes de preservación por parte de las autoridades gubernamentales vía email, donde generalmente se adjunta copia escaneada del oficio u otro documento de solicitud firmado. En las páginas de estas redes, generalmente consta la dirección de email para enviar estos pedidos.

En los casos de delitos cometidos a través de *sitios web* (sitios electrónicos), tales como subastas falsas, venta de

medicamentos prohibidos y crímenes de odio y racismo, se recomienda utilizar las plataformas públicas de preservación de contenido.

Saber más

El más conocido de ellos es Wayback Machine (www.archive.org/web), un banco de datos digital creado por la organización sin fines de lucro Internet Archive y que ha archivado más de 475 mil millones de páginas de la World Wide Web desde 1996.

El procedimiento de preservación es muy simple, todo lo que los usuarios tienen que hacer es introducir la dirección del *sitio web* investigado en el campo "*browse history*". La plataforma permite a cualquier persona acceder al contenido de los *sitios web* archivados allí.

Clase 4 – Otros Medios de Preservación de la Evidencia Digital

CONTEXTUALIZANDO...

La **preservación de los vestigios** constituye uno de los **pasos más importantes** de la investigación cibernética, ya que es el garante de su propia existencia. Sin embargo, hay que tener en cuenta que en la mayoría de las situaciones es la propia víctima la que se enfrenta con el vestigio y tiene la rara oportunidad de conservarlo.

En esta clase entenderemos cómo funciona el procedimiento de denuncia de un crimen cibernético, al considerar las aplicaciones y plataformas que no cuentan con asistencia específica para los procesos de investigación.

PROCEDIMIENTOS DE DENUNCIA DE DELITOS CIBERNÉTICOS

Algunas redes sociales no tienen plataformas o no responden a las solicitudes de asistencia de investigaciones enviadas por los agentes vía email, especialmente aquellas provenientes del exterior. No son raros los casos en los que el agente policial no encuentra rastros de un crimen cometido en *internet*, lo que probablemente provoque que su investigación no sea exitosa.

En la Práctica

En este sentido, ¿cómo puede la víctima proceder frente a un crimen cibernético?

Una vez se tenga conciencia del delito, la víctima o interesados deberán dirigirse de inmediato a una **notaría** de su ciudad y solicitar que se redacte un **acta notarial**.

A través de esto, el notario elabora un instrumento público formalizado por la narrativa fiel de todo lo que ha verificado a través de sus propios sentidos, sin emitir opinión, juicio de valor o conclusión, que servirá como prueba preconstituida para su uso en el ámbito policial y judicial.

Figura 24: Formalización de la denuncia del crimen. **Fuente:** labSEAD-UFSC (2020).

En la verificación de los hechos publicados en la red de *internet*, el notario o encargado ingresará a la red social o al *sitio web* a través de su propia computadora en la Notaría.

> Después de comprobar el contenido, el notario describirá los elementos gráficos y sonoros, así como replicará el contenido escrito con las mismas palabras. El acta notarial deberá contener información sobre la fecha y hora de las publicaciones y su acceso.

Otro medio adecuado para la preservación es el certificado de un agente policial, un servidor dotado de fe pública.

Figura 25: El certificado es también una formalización de la denuncia del delito. **Fuente:** Pixabay (2020), adaptado por labSEAD-UFSC (2020).

Además de las actas, también contendrá las direcciones a las que se ha accedido, descripción del contenido y datos relacionados con fechas y horas. Otros agentes de la unidad de policía, como el investigador, también pueden dar fe de los hechos, pero en forma de informe, en el que detalla, además de los hechos, las diligencias empleadas en el caso.

Saber más

Algunos programas de distribución gratuita, como HTTrack Website Copier, por ejemplo, son capaces de copiar completamente el contenido de los *sitios web* y almacenarlos en el directorio elegido por el usuario.

Haz clic en el *link* para consultar: https://www.httrack.com/.

Aplicaciones como esta se pueden utilizar como herramientas de preservación, pero también se recomienda utilizar otras herramientas útiles para demostrar la integridad del vestigio, como es el caso de aquellas que envían el archivo a una función *hash*, como ***MD5Summer.***

Programa informático de código abierto que permite comprobar la integridad de los archivos transmitidos a través de una red, como por ejemplo internet, para así garantizar que los datos no fueron corrompidos durante la transferencia.

En la práctica, es muy común que las personas realicen el procedimiento de captura de pantalla de una computadora o *screenshot*, en caso de que se trate de un *smartphone*, para almacenar una imagen que demuestre un hecho ocurrido en el ciberespacio.

> **¡ATENCIÓN!**
> Este no es el mejor medio de preservación, si tenemos en cuenta la dificultad de verificar la autenticidad e integridad del vestigio.

En algunas situaciones, la captura omite elementos importantes para la investigación del delito, tales como: dirección electrónica, fechas y horas.

Sin embargo, en caso de que este sea el único registro del hecho existente, por regla general se agrega a la colección probatoria, en la que se analizará con otros elementos de condena.

Como vimos anteriormente, la preservación del vestigio es indispensable para la investigación de un delito. Este es el paso que asegurará la consistencia de los demás, tanto desde el punto de vista técnico, es decir, la calidad de la prueba, como legal, relacionado con la validez de la prueba.

Por esta razón, se mencionaron los principales medios de recopilación y almacenamiento de vestigios, a pesar de la metodología de cadena de custodia descrita en la Ley 13.964 de 2019, que modificó el Código Procesal Penal de Brasil.

Clase 5 – Recopilación de Información Adicional y Entrevista Especializada

CONTEXTUALIZANDO...

Debido a las características dinámicas de los delitos cibernéticos estudiadas hasta ahora, podemos admitir la importancia de preservar los vestigios digitales. Sin embargo, los momentos iniciales que siguen al crimen cuentan con muchos elementos materiales e información que están relacionados con los insumos digitales.

En esta clase, comprenderemos cómo la relación de la víctima con el oficial de seguridad pública es indispensable, tanto para dar el apoyo necesario a la víctima del delito cibernético, como para recopilar la información necesaria para llevar a cabo la investigación penal.

ATENCIÓN A LAS VÍCTIMAS

La noticia de la consumación de un delito llega a la unidad de policía de diversas maneras, incluso a través de un oficio del **Ministerio Público** y otros órganos externos.

> La denuncia de un delito cibernético que llega a través de documentos es a menudo precaria, porque trae sólo los elementos mínimos que caracterizan al crimen.

Por otro lado, cuando la víctima se presenta al órgano competente para realizar la denuncia, es inevitable reconocer que existe una oportunidad sustancial para la presentación de pruebas. Esto se debe a que el entrevistador, es decir, la persona responsable del cuidado del caso tiene una gran oportunidad de acortar el tiempo de su investigación, ya que allí se pueden proporcionar los datos que se necesitan.

Es innegable que el entrevistado posee y guarda una gran cantidad de datos que son extremadamente útiles para el caso, y la experiencia policial señala tres razones por las que esta información es ocultada por el entrevistado.

La imagen a continuación presenta las principales razones.

Figura 26: Razones principales para ocultar información.
Fuente: labSEAD-UFSC (2020).

En cuanto a la vergüenza de exponer su intimidad, la desconfianza del ciudadano en lo que respecta al apoyo que el Estado le brindará en su caso particular es muy común.

> Esta incredulidad es la razón principal por la que la persona informa solo lo mínimo necesario. Existe el concepto preconcebido de que la exposición total puede ser incluso más perjudicial que la no aclaración del delito.

Aquí entra el miedo por parte de la víctima de que sea imputada por el crimen, un pensamiento común y perjudicial para el proceso de investigación. **Podemos diagnosticar este tipo de comportamiento como un problema estructural de las unidades de atención a víctimas de delitos**.

Las fuerzas policiales deben mejorar su estructura en lo que respecta a la formación de sus profesionales y su logística, para que escuchen a las víctimas con técnicas profesionales y de recepción.

Sólo de esta forma podremos superar los estigmas que aún fortalecen la idea de que la policía está alejada del ciudadano.

En la Práctica

En los casos de venganza digital, o *revenge porn*, a menudo es la propia víctima quien envía videos íntimos a su pareja o cónyuge. El oficial sabe que el archivo fue producido exclusivamente por la víctima, por ejemplo a través de su teléfono celular, y que sólo se envió a su ex pareja.

En este caso, ¿cómo podemos entender a la víctima frente a este crimen?

En el ejemplo anterior, existen algunos elementos que pueden ser evitados por parte del agente. Por lo tanto, se puede afirmar que los detalles relativos a las fechas y el canal de envío de los datos, cifrados o no, pueden limitar el enfoque de la investigación, para no perder tiempo y recursos con representaciones y análisis complejos.

Vale la pena recordar que cuando existe la divulgación de material sin autorización en la red, de ninguna manera se puede caracterizar como culpa exclusiva de la víctima. Por el contrario, veremos en las próximas lecciones que, en el delito de **venganza digital**, la legislación consideró el aspecto de **violación de confianza** como una causa para **aumentar la pena**.

Por lo tanto, este tipo de postura prejuiciosa de un profesional de seguridad pública es considerado **inadmisible**, ya que, en lugar de condenar a la víctima, el profesional debe prestarle total apoyo.

Figura 27: La persona tiene miedo de ser acusada del delito del que es víctima. **Fuente:** Pixabay (2020).

Al ganar la confianza de la víctima, ésta puede dotar a la unidad de datos importantes para la investigación.

Con respecto a la ignorancia de las víctimas sobre la importancia de la información, muchas ocultan información simplemente porque no saben cuán importante es.

Es muy común, por desgracia, situaciones en las que las personas toman capturas de pantalla de *smartphones* o incluso computadoras de escritorio, almacenan esta imagen y, a continuación, eliminan los mensajes, denuncian al proveedor o eliminan sus cuentas.

Figura 28: Las capturas de pantalla no se recomiendan como vestigios de delitos cibernéticos. **Fuente:** Pixabay (2020).

Cuando esto ocurre sin las medidas de preservación anteriormente expuestas, la investigación puede estar condenada al fracaso. Se ha demostrado que la captura de pantalla no es el mejor medio y, si no se realiza correctamente, puede que no capture información esencial para la producción probatoria, como la URL, por ejemplo.

> Al igual que con las víctimas que no conocen la importancia de la información, las personas no comparten aspectos importantes sobre el hecho con la unidad de atención. Ante esta situación natural, corresponde al profesional, a través de preguntas, buscar esta información.

De hecho, en todos los casos, es importante aplicar una estrategia a la entrevista, para que se extraigan los insumos importantes de la investigación, pero con un método capaz de ganarse la confianza de la víctima.

Figura 29: Apoyo a las víctimas. **Fuente:** Shutterstock (2020).

Esto se basa en la premisa de que, en algunos casos, no todos los datos serán presentados por la persona de una sola vez, principalmente por razones emocionales. Otro factor de extrema atención por parte de quien realiza la atención es el riesgo de revictimización del ciudadano.

Revictimización

En **casos más delicados**, como atención a mujeres víctimas de violencia psicológica a través de la red o niños abusados virtualmente, se debe **evitar la repetición de preguntas sobre detalles de escenas y hechos más íntimos**, ya que estos recuerdos pueden reanudar sentimientos de profundo sufrimiento para estas personas.

Figura 30: Algunos informes causan molestias a las víctimas. **Fuente:** Pixabay (2020).

En casos de un crimen cibernético cuyo *modus operandi* demuestra uso de alta tecnología, se recomienda que dicha **atención** sea realizada por el **equipo especializado** de la unidad, ya que algunos detalles pueden perderse al momento de registrar una ocurrencia o boletín policial.

DELITOS CONTRA CORPORACIONES

En los casos de delitos contra corporaciones, en los que los servidores de datos se vean afectados, el administrador de la persona jurídica debe estar acompañado por un director técnico o representante de la empresa contratada para proporcionar seguridad de la información.

En estas situaciones, la presencia de estas personas es fundamental, al considerar que se les preguntará sobre aspectos importantes, entre los que se encuentran:

Figura 31: Informaciones que deben ser recopiladas por el equipo de seguridad.
Fuente: labSEAD-UFSC (2020).

Entre los puntos planteados anteriormente, se destaca la importancia de **adherirse a las condiciones de preservación de los vestigios**. En el caso de las empresas que son víctimas, éstas suelen proporcionar un informe técnico sobre el incidente de seguridad.

> Este documento es elaborado por particulares o empresas privadas que poseen conocimientos técnicos, pero desconocen los procedimientos de la cadena de custodia, descritos actualmente en la ley.

Su uso en el cuerpo probatorio puede ser cuestionado por la defensa de la parte investigada cuando no cumpla con los requisitos legales. Por lo tanto, es preferible que los órganos competentes para la investigación se dirijan al lugar del crimen y lleven a cabo el procedimiento adecuado para la recopilación de vestigios.

Referencias

BARRETO, A. G.; BRASIL, B. S. **Manual de investigação cibernética**: à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941.** Brasília, DF: Presidência da República, [2019a]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 28 jul. 2020.

BRASIL. Supremo Tribunal Federal. **Conflito de Competência n.º 40.569-SP**. Relator: José Arnaldo da Fonseca. 10 mar. 2004. Brasília, DF, 2004. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/7380604/conflito-de-competencia-cc-40569-sp-2003-0187145-1/inteiro-teor-13043137. Acesso em: 30 jul. 2020.

FLATICON. [*S.l.*], 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 16 jul. 2020.

FEERPIK. [*S.l.*], 2020. Disponível em: https://br.freepik.com/. Acesso em: 5 ago. 2020.

LOCARD, E. **A investigação criminal e os métodos científicos**. São Paulo: Saraiva, 1939.

PIXABAY. [*S.l.*], 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 16 jul. 2020.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 14 jul. 2020.

MÓDULO 4

LEGISLACIÓN VIGENTE RESPECTO A LOS CRÍMENES ELECTRÓNICOS EN BRASIL

Presentación

La legislación que rige el fenómeno del crimen electrónico en Brasil es bastante reciente en comparación con otras leyes que componen el sistema legal brasileño.

Varios países impulsaron iniciativas legislativas sobre delitos cibernéticos mucho antes que Brasil, por lo que la legislación brasileña está influenciada por diversas medidas legislativas que fueron adoptadas en otros países.

A partir de este punto, en este módulo, aprenderemos más sobre la legislación que rige los crímenes digitales en Brasil y resaltaremos la importancia de su comprensión para la investigación y lucha contra el crimen.

OBJETIVOS DEL MÓDULO

Conocer la base jurídica de la **legislación internacional** y la **brasileña** en relación con los crímenes electrónicos cometidos en el Brasil.

ESTRUCTURA DEL MÓDULO

- **Clase 1 –** Legislación Internacional.
- **Clase 2 –** Marco Civil de Internet.
- **Clase 3 –** Delitos Cibernéticos previstos en la Legislación Brasileña.

Clase 1 – Legislación Internacional

CONTEXTUALIZANDO...

Como ya vimos anteriormente, la legislación brasileña sobre crímenes electrónicos está influenciada por diversas medidas legislativas que fueron adoptadas por otros países, dando oportunidad así, a las que seguidamente fueron impulsadas en el país.

Por lo tanto, antes de empezar con el estudio de las normas brasileñas sobre delitos cibernéticos, es necesario conocer algunas leyes extranjeras que son una referencia mundial en este tema.

¡Adelante!

EL PLAN INTERNACIONAL

A nivel internacional, la legislación relacionada con los crímenes electrónicos se observa en los siguientes países: Alemania, España, Austria, Chile, Francia, Estados Unidos, Italia, Venezuela, México, Bolivia, Costa Rica, Perú, Ecuador, Gran Bretaña, Portugal y Japón, entre otros.

Figura 1: Legislación relacionada con los crímenes electrónicos en todo el mundo. **Fuente:** Pixabay (2020).

En este universo de leyes internacionales que abordan los delitos cibernéticos, se destacan dos instrumentos: el Convenio de Budapest, sobre Ciberdelincuencia, y el Reglamento General de Protección de Datos (RGPD) vigente en Europa.

A continuación, estudiaremos más sobre estos instrumentos.

Convenio de Budapest sobre el delito cibernético

El **Convenio de Budapest** sobre Ciberdelincuencia, también conocido como CETS 185, fue firmado por el Consejo de Europa en 2001 y entró en vigor en 2004.

> Consiste en un tratado internacional sobre derecho penal y derecho procesal penal, que tiene por objeto definir un trato armonioso que siempre debe darse en la persecución penal de los crímenes digitales a nivel europeo.

El preámbulo del Convenio de Budapest explica que el mencionado instrumento busca adoptar **"una política criminal común, con el objetivo de proteger a la sociedad contra la delincuencia en el ciberespacio, principalmente a través de la adopción de legislación adecuada y de la mejoría en la cooperación internacional."** (traducción nuestra)

El Convenio de Budapest sobre Ciberdelincuencia establece, en la sección 1 (Derecho Penal Material) del capítulo II (Medidas a tomar a nivel nacional), el deber de los Estados Parte en tipificar determinadas conductas en el contexto de delitos cibernéticos.

Vamos a conocer estas conductas en la siguiente imagen.

1

Acceso ilegítimo– Se trata de la conducta de acceso intencional e ilegítimo a la totalidad o a una parte de un sistema informático con la violación de medidas de seguridad, con la intención de obtener datos informáticos u otras intenciones ilegítimas, o relacionada con un sistema informático conectado a otro sistema informático. Este crimen es similar al delito de invadir un dispositivo informático previsto en el Art.154-A del Código Penal de Brasil.

2

Intercepción ilegítima– Se trata de la interceptación intencional e ilegítima de datos informáticos efectuada por medios técnicos, en transmisiones no públicas. Este delito es similar al delito de interceptación ilícita de comunicaciones telefónicas, informáticas o telemáticas previsto en el artículo 10 de la Ley Nº 9.296/1996.

3

Interferencia en los datos – Se trata del acto de dañar, borrar, deteriorar, alterar o eliminar intencional e ilegítimamente datos informáticos. Brasil tiene dos tipos penales similares a este, a saber, los delitos previstos en los artículos 313-A y 313-B del Código Penal (CP) brasileño, en los que se prevén los delitos de inserción de datos falsos en sistema de información y la modificación o cambio no autorizados del sistema de información, respectivamente.

4

Interferencia en sistemas – Se trata de la obstrucción grave, intencional e ilegítima, el funcionamiento de una computadora, a través de la introducción, transmisión, daño, eliminación, deterioro, modificación o eliminación de datos informáticos. Una vez más, existe un tipo penal similar al del ordenamiento jurídico brasileño que es el delito de interrupción o perturbación de servicio telegráfico, telefónicos, informáticos, telemáticos o de información útil previstos en el art. 266 de CP de Brasil.

Figura 2: Conductas consideradas delitos cibernéticos, de acuerdo con el Convenio de Budapest sobre Ciberdelincuencia. **Fuente:** labSEAD-UFSC (2020).

Teniendo en cuenta lo anterior, es interesante que conozcamos el Código Penal (CP) Brasileño y la Ley 9.296/1996 para asegurarnos de tener una inmersión real en el contenido y mejorar nuestros conocimientos en el área.

Saber más

Para conocer el Código Penal Brasileño completo, haz clic en el *link*: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm

Para conocer, de forma íntegra, la Ley 9.296/1996, haz clic en el *link*: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm

Además de las conductas consideradas delitos cibernéticos, de acuerdo con el Convenio de Budapest sobre Ciberdelincuencia que ya vimos, también se destaca la conducta de **"Uso Abusivo de Dispositivos"**. En este caso, el crimen se entiende como la posesión con intención de uso, producción, venta, obtención para su utilización, importación, distribución u otras formas de suministro de dispositivos y accesos.

Veamos, a continuación, lo que configura cada aspecto.

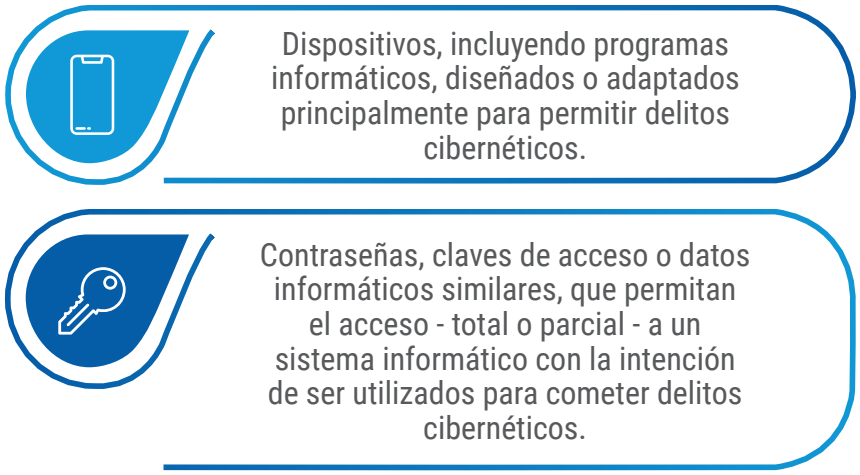


Figura 3: La conducta de uso abusivo de dispositivos. **Fuente:** labSEAD-UFSC (2020).

En este caso, la ley brasileña apunta a un crimen similar, que es el crimen previsto en el **§ 1° del Art. 154-A del Código Penal Brasileño:**

> *Dañar, distribuir, vender o difundir un dispositivo o programa informático con el fin de permitir la práctica de la intrusión en dispositivos informáticos.*

También se consideran otras conductas como delitos cibernéticos, de acuerdo con el Convenio de Budapest sobre Ciberdelincuencia.

Eso es lo que conoceremos a continuación.

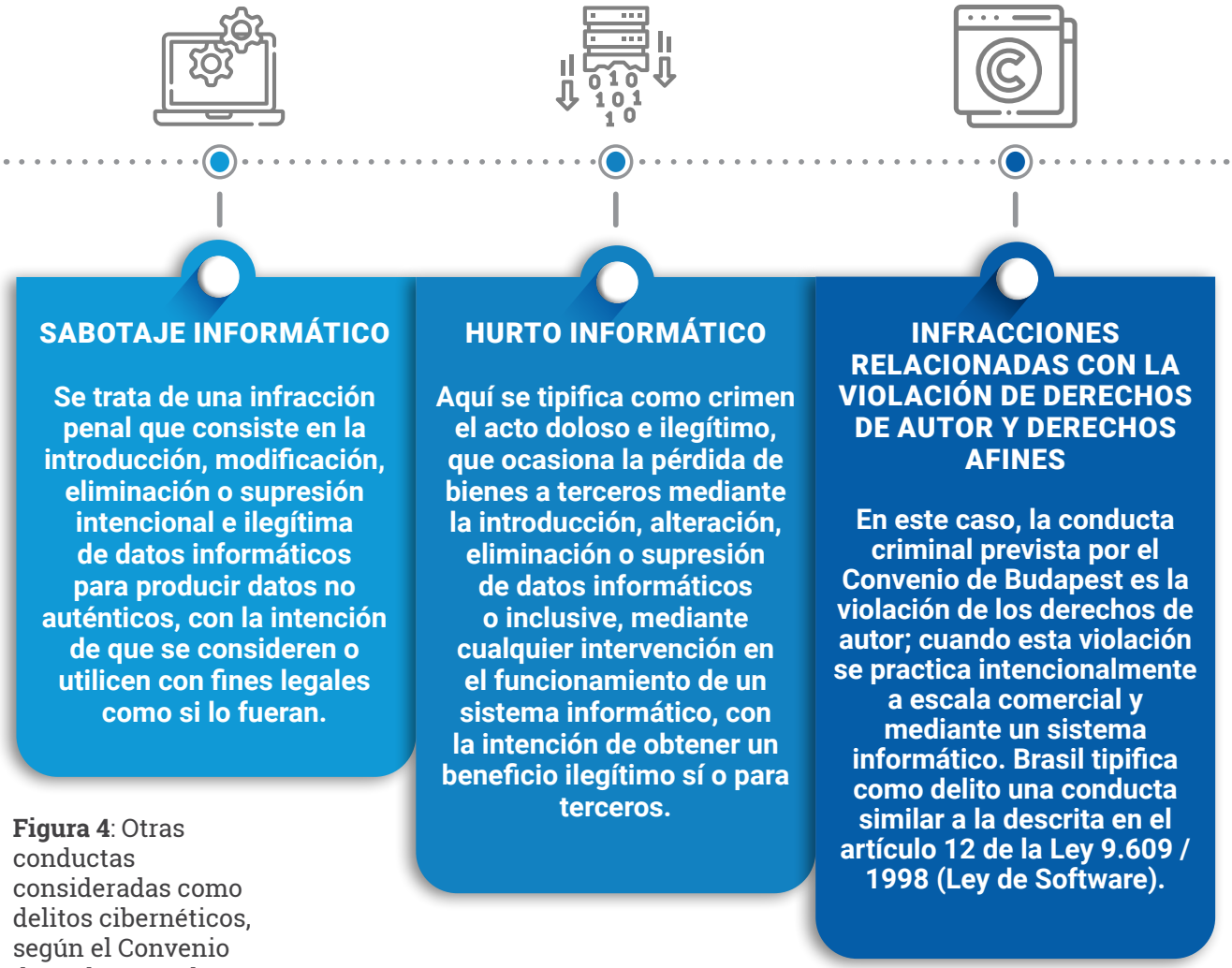


Figura 4: Otras conductas consideradas como delitos cibernéticos, según el Convenio de Budapest sobre Ciberdelincuencia. **Fuente:** labSEAD-UFSC (2020).

Acerca de la conducta de **sabotaje informático** que acabamos de conocer -en la imagen anterior- cabe mencionar que, si bien este delito puede confundirse con el delito de "injerencia de datos", previsto en la Convención de Budapest, o con los delitos de los artículos 313- A y 313-B del Código Penal Brasileño, éste delito concierne específicamente en

la producción y uso de datos falsos, por lo tanto, no existe un equivalente riguroso en el derecho penal brasileño. Conductas como esta, en Brasil, serían tipificadas como *falsedad ideológica* o *falsa identidad*, según el contexto.

En lo que se refiere a la conducta de **hurto informático**, podemos decir que es bastante similar al tipo delictivo de "Invasión de Dispositivo Informático" previsto en el Art. 154-A del CP brasileño.

Veamos lo que establece este artículo del CP brasileño, en la siguiente imagen.

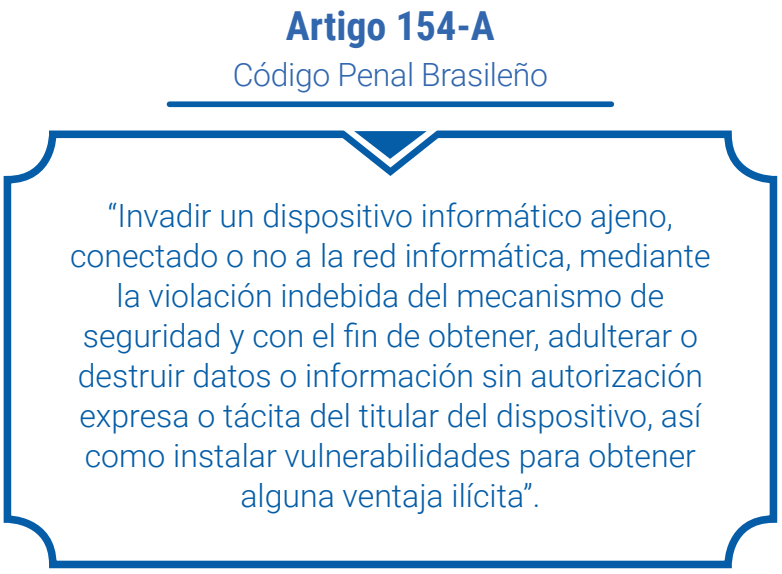


Figura 5: Art. 154-A del Código Penal de Brasil, relativo a la conducta de intrusión en dispositivos informáticos. **Fuente:** labSEAD-UFSC (2020).

Finalmente, cabe mencionar la conducta de **"Infracciones relacionadas con la Pornografía Infantil"**. En este caso, el Convenio de Budapest hace referencia a una lista de conductas clasificadas que incluyen algunas infracciones generales. Las cuales conoceremos a continuación.

1. Producir pornografía infantil para su difusión a través de un sistema informático.
2. Ofrecer o publicitar pornografía infantil a través de un sistema informático.
3. Difundir o transmitir pornografía infantil a través de un sistema informático.

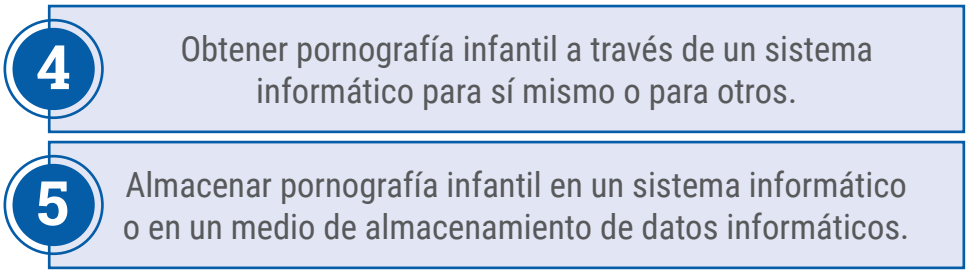


Figura 6: Infracciones relacionadas con la pornografía infantil, de conformidad con el Convenio de Budapest sobre Ciberdelincuencia.
Fuente: labSEAD-UFSC (2020).

Estos delitos relacionados con la pornografía infantil son muy similares a los artículos 240 a 241-E del Estatuto de la Niñez y la Adolescencia (ECA) de Brasil.

En la Práctica

Para reflexionar...

En vista de ello, podemos observar, en comparación con la conducta relacionada con el Código Penal, que muchos delitos cibernéticos tipificados por la legislación brasileña se inspiran o reflejan crímenes señalados por la Convención de Budapest.

Aunque el Convenio de Budapest sobre Ciberdelincuencia sea considerado un instrumento de excelencia, Brasil, por iniciativa propia, no puede adherirse a él. No obstante, el artículo 37 del Convenio estipula que el Comité de Ministros del Consejo de Europa puede, después de consultar a los Estados contratantes del Convenio y obtener un acuerdo unánime, invitar a cualquier Estado que no sea miembro del Consejo y que no haya participado en su preparación, adherirse al Convenio.

Por lo tanto, es posible que algún día, por medio de una invitación, Brasil se convierta en un país signatario de dicho Convenio.

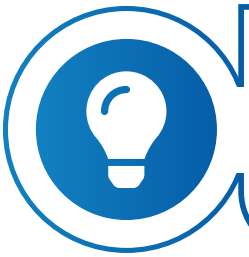
Red 24/7

Aún dentro del contexto de la Convención de Budapest sobre Ciberdelincuencia, podemos destacar su artículo 35, donde prevé la figura de la **Red 24/7**.

De conformidad con este artículo, cada uno de los signatarios del Convenio debe designar un punto de contacto disponible las 24 horas del día, los siete días de la semana, a fin de asegurar la prestación de asistencia inmediata a las investigaciones o procedimientos relacionados con delitos penales ligados a datos y/o sistemas informáticos, o que requieran recolectar evidencia, en forma electrónica, de un delito.

> Aunque Brasil no es signatario del Convenio de Budapest, la Policía Federal de Brasil dispone de un instrumento similar. La Policía Federal forma parte del 24/7 de varios países que integran unidades de investigación de delitos cibernéticos.

A través de esta red, por ejemplo, existe la posibilidad de solicitar la preservación inmediata de datos en otros países.



Saber más

Si es necesario para tu investigación, ten en cuenta la dirección de correo electrónico para solicitudes a la Red 24/7 de la Policía Federal de Brasil: cybercrime_brazil_24x7@dpf.gov.br

Uno de los instrumentos internacionales que contempla el crimen cibernético es el Convenio de Budapest sobre Ciberdelincuencia. Ahora que conocemos un poco más la legislación que lo rige, entenderemos mejor el segundo instrumento internacional que existe en este contexto, el Reglamento General de Protección de Datos (RGPD), vigente en Europa.

Reglamento general de protección de datos — GPDR

El 25 de mayo de 2018 entró en vigor el General Data Protection Regulation (GDPR), que puede traducirse como “Reglamento General de Protección de Datos”.

> La GDPR es una legislación de la Unión Europea que establece normas generales sobre la forma en la cual las empresas y los organismos públicos deben manejar los datos personales de los usuarios de *internet*.

El GDPR, o RGPD en español, creó diversos derechos para los usuarios de *internet* con el fin de proteger su privacidad. Estos derechos principales están relacionados con el derecho del usuario de *internet* a saber cuáles de sus datos han sido tomados por empresas y la finalidad de su uso.

Veamos esos derechos de los usuarios en la imagen a continuación:

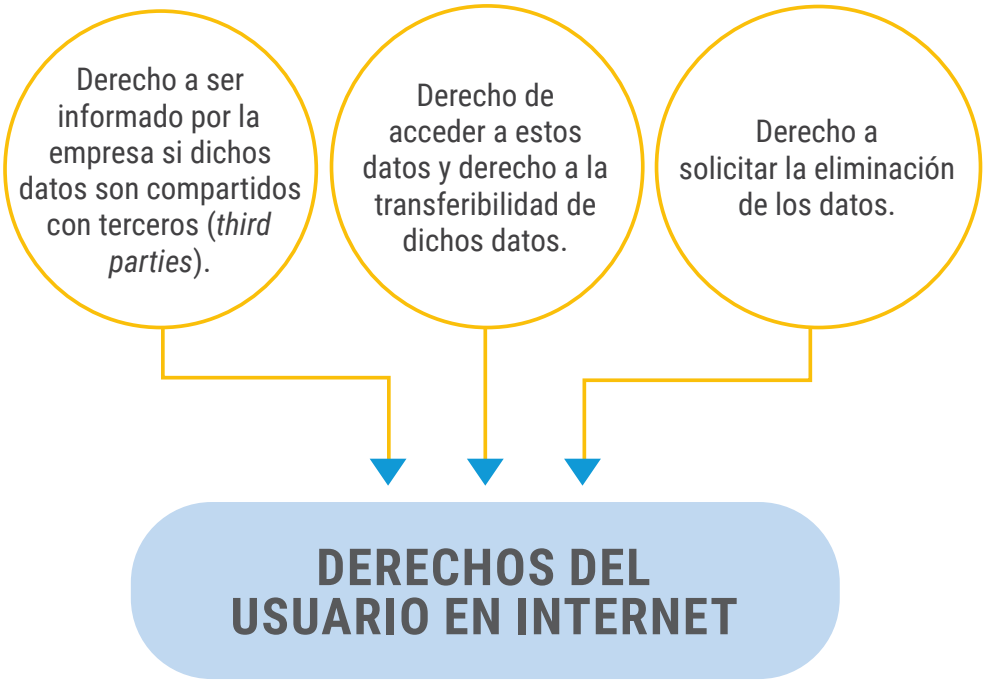


Figura 7: Derechos de usuarios en *internet*, según el Reglamento General de Protección de Datos. **Fuente:** labSEAD-UFSC (2020).

Junto a estos derechos, el GDPR creó obligaciones para las empresas que operan en medios digitales; como **la obligación de notificar a los usuarios sobre la transgresión de sus datos dentro de las 72 horas siguientes al hecho**, por ejemplo. El incumplimiento por parte de las empresas de estas obligaciones puede acarrear desde advertencias hasta multas que pueden alcanzar los 20 millones de euros o el 4% de los ingresos de la empresa.

Es decir, el GDPR es una iniciativa legislativa de la Comunidad Europea y que tiene como objetivo proteger al usuario de *internet* y su privacidad.

> Aunque el RGPD no sea una ley penal; la violación de sus términos tiende estar relacionada con la práctica de crímenes, y por ello es importante que los representantes del sistema de justicia penal que intervienen en los crímenes electrónicos conozcan su existencia.

En este sentido, desde que entró en vigor en mayo de 2018, el RGPD estipula que las empresas deben informar a la autoridad cibernética de protección de datos personales, si ha habido una violación de datos, en inglés, *data breach*, en hasta **72 horas**.

En particular, según el GDPR, cuando las empresas se enfrentan a un posible delito cibernético contra ellas, deben evaluar la violación de datos y los posibles daños. **Así, como realizar diagnósticos para determinar si los datos personales se han visto comprometidos.**

En este caso, las autoridades locales de protección de datos deben ser informadas en un plazo de 72 horas, y el informe del incumplimiento debe contener: **el tipo de ataque, la cantidad de datos personales afectados, las acciones tomadas y previstas para eliminar consecuencias o reducir el impacto. Si la empresa atacada no cumple con estas disposiciones del RGPD, se verá obligada a pagar multas.**

> En caso de infracción grave, además de la autoridad cibernética de protección de datos personales, también deben ser informados los titulares de datos personales cuya información se haya visto comprometida.

En relación con este tema, el General Data Protection Regulation, introdujo un enfoque correlacional para aplicación de multas, lo que significa que la gravedad de la infracción determinará la sanción. Dentro del GDPR, hay dos formas de aplicar una multa contra la empresa.

¡Conozcámosla!

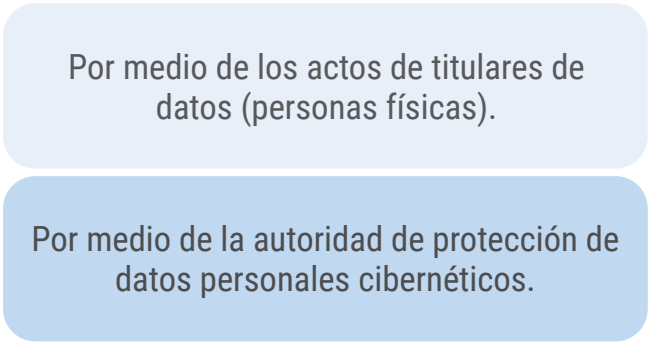


Figura 8: Sanciones aplicadas en las empresas por resultado de multas del GDPR. **Fuente:** labSEAD-UFSC (2020).

La multa máxima a la que deberá hacer frente una empresa es del 4% de su facturación de negocios anual global o de 20 millones de euros, lo que sea mayor.

A modo de ejemplo, cuando la aerolínea British Airways fue blanco de un ataque cibernético en septiembre de 2018, sólo le tomó un día informar a sus clientes que se habían robado información de unas 380.000 transacciones de reserva habían sido sustraídas, incluidos números de tarjetas bancarias, fechas de caducidad y códigos CVV.

Estos datos se obtuvieron a través de un ***script*** malicioso creado para robar información financiera, este *script* que se ejecutaba en la página de pago de British Airways, antes de que se enviara la información de pago. Como resultado, según las disposiciones del GDPR, British Airways recibió una multa de £ 183 millones ($ 229 millones).

Script – conjunto de instrucciones para que una función sea ejecutada en una aplicación particular.

Por lo tanto, aunque el GDPR no prevé crímenes y no tiene disposiciones penales o procesales, el crimen cibernético sin dudas está estrechamente relacionado con los dispositivos

del GDPR, o RGPD en español. Esto se debe a que la práctica del crimen cibernético implica una violación de la privacidad, lo cual es extensa y profundamente contemplado por el GDPR.

Hasta ahora, ya conocemos dos importantes instrumentos internacionales que son puntos de referencia mundiales, en lo relacionado con los crímenes o delitos cibernéticos. En la siguiente clase, daremos seguimiento a las normas brasileñas relativas a los crímenes digitales.

Clase 2 – Marco Civil de Internet

CONTEXTUALIZANDO...

Para conocer las normas brasileñas en torno a los delitos cibernéticos, debemos aprender más sobre la **Ley 12.965/2014** (disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm), que caracteriza el Marco Civil de Internet en Brasil, y sus disposiciones con mayor relevancia para la Seguridad Pública y para la investigación de delitos cibernéticos.

LEY 12.965/2014

El Marco Civil de Internet (Ley 12.965/2014) es el decreto legislativo que regula el uso de Internet en Brasil, proporcionando principios, garantías, derechos y deberes para quienes utilizan la red, así como presenta directrices e hitos para la actuación del Estado.

Aunque es una ley relativamente extensa, de acuerdo con el Fiscal Regional de la República en Brasilia, Vladimir Aras, el Marco Civil de Internet tiene cuatro ejes. Vamos a conocerlos a continuación.

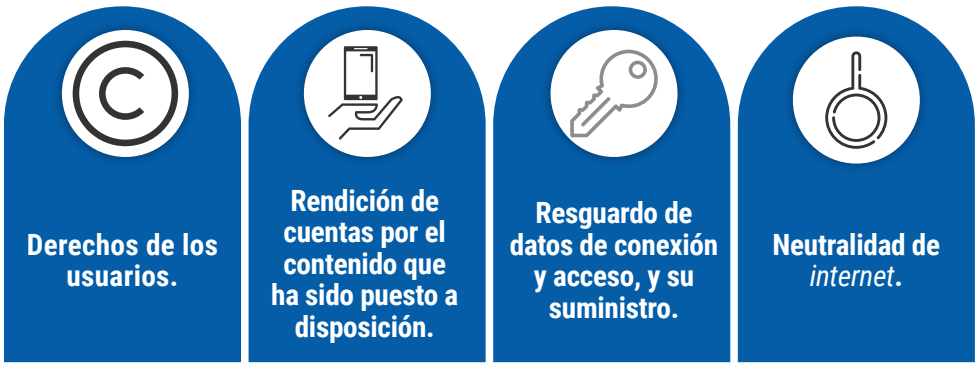


Figura 9: Ejes del Marco Civil de Internet en Brasil, según Vladimir Aras. **Fuente:** labSEAD-UFSC (2020).

Según Vladimir Aras, estos ejes tienen implicaciones criminales, excepto por el eje de neutralidad de la red.

El Marco Civil de Internet establece, en su artículo 13, conceptos fundamentales, sin los cuales sus disposiciones

no podrían ser entendidas en su totalidad. Conoce estos conceptos fundamentales analizando la siguiente imagen:

1. **Internet -** sistema compuesto por un conjunto de protocolos lógicos, estructurados a escala mundial, para uso público e irrestricto, con el fin de permitir el intercambio de datos entre terminales diferentes a través de redes.

2. **Terminal -** computador o cualquier dispositivo que se conecte a *internet*.

3. **Dirección de protocolo de *internet* (dirección IP) -** código asignado a un terminal de una red para permitir su identificación, éste es definido de acuerdo con parámetros internacionales.

4. **Administrador del Sistema Autónomo -** persona física o jurídica que gestiona determinadas direcciones IP, y el respectivo sistema autónomo de enrutamiento, debidamente registrado en la entidad nacional responsable de registro y distribución de direcciones IP geográficamente relacionadas con el país.

5. **Conexión a *internet* -** habilitación de un terminal para enviar y recibir paquetes de datos a través de *internet*, asignando o autenticando una dirección IP.

6. **Registro de conexión-** conjunto de información relativa a la fecha y hora de inicio y finalización de una conexión a *internet*, su duración y la dirección IP utilizada por el terminal para enviar y recibir los paquetes de datos.

7 **Aplicaciones de *internet* -** conjunto de funcionalidades a las que se puede acceder a través de un terminal conectado a *internet*.

8 **Registros de acceso a las aplicaciones desde *internet* -** conjunto de información relativa a la fecha y hora de uso de una determinada aplicación de *internet*, a partir de una determinada dirección de IP.

Figura 10: CConceptos fundamentales del Marco Civil de Internet. **Fuente:** labSEAD-UFSC (2020).

En el artículo 4 del Marco Civil de Internet, se estableció la creación de órganos específicos de la policía judicial para combatir los crímenes electrónicos, es decir, **comisarías especializadas**. De acuerdo con este mandamiento legal, algunos estados brasileños adoptaron comisarías especializadas en la investigación de delitos cibernéticos. A continuación, veamos cuáles son.

Figura 11: Estados brasileños con comisarías especializadas. **Fuente:** labSEAD-UFSC (2020).

Desde la perspectiva de la investigación de delitos cibernéticos, el tema principal que el Marco Civil de Internet aborda está relacionado con **la custodia y disponibilidad de datos y contenidos suministrados para realizar registros**.

> Lo que cualquier investigación de delitos cibernéticos busca es que empresas de aplicaciones de *internet* y proveedores de conexión a *internet* proporcionen datos a la policía de investigación (Policía Civil y Policía Federal) para que la investigación pueda llegar a los autores de los delitos.

Pues bien, el Marco Civil de Internet regula este tema, principalmente, estipulando normas sobre el tiempo en que estas empresas deben guardar los datos y en qué condiciones las empresas deben proporcionar estos datos a la policía investigadora.

Con respecto a las disposiciones del Marco Civil de Internet, es importante entender que estas regulan el almacenamiento de datos de registros, bien sea registros de conexión (IPs) y contenido por empresas de aplicaciones de *internet* (Facebook, Instagram, Uber, Nubank etc.) y proveedores de conexión (Net, Vivo, Claro, Oi, Tim, etc.) y en qué condiciones estas empresas deben entregar estos datos a la Policía Civil y a la Policía Federal.

La primera disposición del Marco Civil de Internet relativa a datos de registros, datos de contenido y registros de conexión (IP) se refiere al período de almacenamiento de dichos datos por las empresas de aplicaciones de *internet* y proveedores de conexión.

En la siguiente imagen, observamos lo que establecen los artículos 13 y 15 de Marco Civil de Internet sobre este período de almacenamiento de datos.

Figura 12: Período de custodia de datos por empresas y proveedores de aplicaciones. **Fuente:** labSEAD-UFSC (2020).

En este contexto, imaginemos una investigación sobre un perfil falso de Facebook que cometió delitos contra el honor de varias víctimas en un entorno virtual. Si la investigación demora más de seis meses en solicitar a Facebook los datos de dicho usuario (más adelante veremos cómo el Marco Civil de Internet aborda la cuestión de la solicitud de dato), Facebook no tiene ninguna obligación legal de almacenar los datos o proporcionarlos a la Policía Civil o a la Policía Federal.

Asimismo, si, por cualquier motivo, los organismos investigadores solicitan registros de conexión (IPs) a proveedores de conexión (Net, Vivo, Claro, Oi, Tim etc.) y estas IP son "antiguas", es decir, están relacionadas con hechos que ocurrieron hace **más de un año**, los proveedores de conexión **ya no tienen la obligación de mantener almacenados estos datos.**

Por lo tanto, Marco Civil de Internet prevé plazos muy cortos para la obligación de almacenamiento de datos. Estos plazos comúnmente pueden vencerse en medio de la investigación de crímenes digitales, que pueden durar mucho más de un año.

Pero, ¿cuál es la solución?

La salida que propone el Marco Civil de Internet es el mecanismo de **preservación de datos**.

Si bien el Marco Civil de Internet requiere que las empresas de *internet* y los proveedores de servicios de *internet* almacenan datos por períodos cortos, por otro lado, prevé (Art. 13, § 2º, y art. 15, § 2º) la figura de la solicitud de conservación de datos.

> Esta solicitud consiste en la posibilidad de que la autoridad policial o administrativa o el Ministerio Público soliciten cautelarmente que los datos de registro, los datos de contenido o los registros de conexión se almacenen durante más de un año (para los proveedores de acceso) o seis meses (para los proveedores de solicitudes).

De esta forma, para evitar la pérdida de datos que se almacenan sólo durante un año (para proveedores de acceso) o seis meses (para los proveedores de solicitudes), la autoridad policial, administrativa o el Ministerio Público pueden solicitar a los proveedores acceso y proveedores de aplicaciones que conserven por más tiempo estos datos. Como resultado, los proveedores de acceso y los proveedores de aplicaciones conservan estos datos hasta recibir la solicitud por parte de la policía de investigación, Ministerio Público o el Poder Judicial.

Sin embargo, el Marco Civil de Internet establece que, hecha esta solicitud por parte de la autoridad requirente **de que los datos sean conservados por más tiempo del esperado**, la policía de investigación (Policía Civil y Policía Federal) debe, dentro de **sesenta días**, contados de la solicitud, ingresar a los registros con el pedido de autorización judicial.

En el capítulo relativo a la investigación de crímenes electrónicos, se abordarán los procedimientos que deben adoptarse para solicitar la preservación de datos.

Saber más

En cuanto a la custodia y disponibilidad de registros de conexión y acceso a aplicaciones de *internet*, datos personales y el contenido de las comunicaciones privadas, el Marco Civil de Internet establece que se debe considerar la preservación de la intimidad, la privacidad, el honor y la imagen de las partes involucradas directa o indirectamente.

Esto significa que los datos de registro, los registros de conexión o acceso, los datos personales y el contenido de las comunicaciones privadas forman parte del ámbito de protección de la privacidad de las personas y no pueden ser accedidos libremente, ni siquiera por los órganos de persecución penal, como el Ministerio Público, la Policía Civil y la Policía Federal.

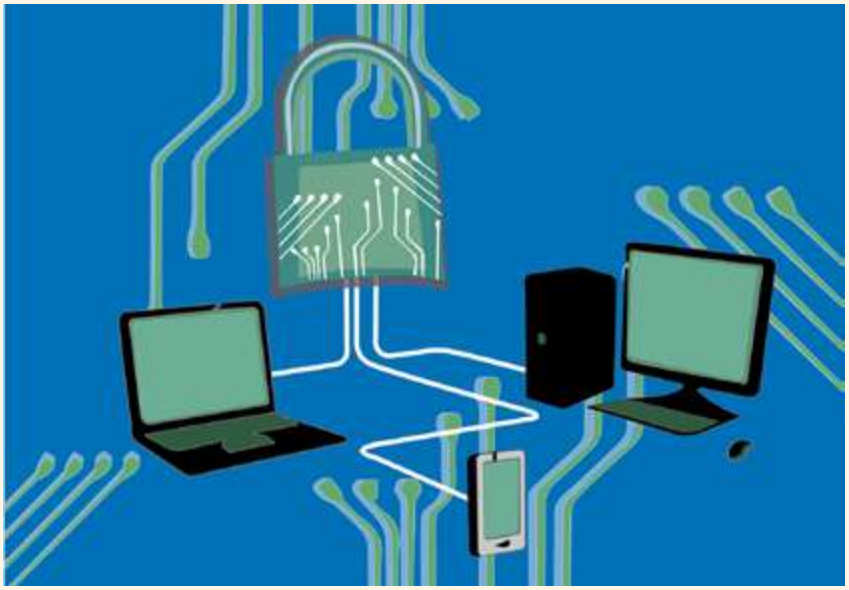


Figura 13: El almacenamiento de datos debe preservar la privacidad de las comunicaciones personales y privadas **Fuente:** Pixabay (2020).

A continuación, el Marco Civil de Internet separa estos datos en dos categorías, según el grado de privacidad personal implicado. Por lo tanto, el documento hace una incisión y dispensa diferentes formas de tratar los datos generales y datos de registro.

Veamos la siguiente imagen:

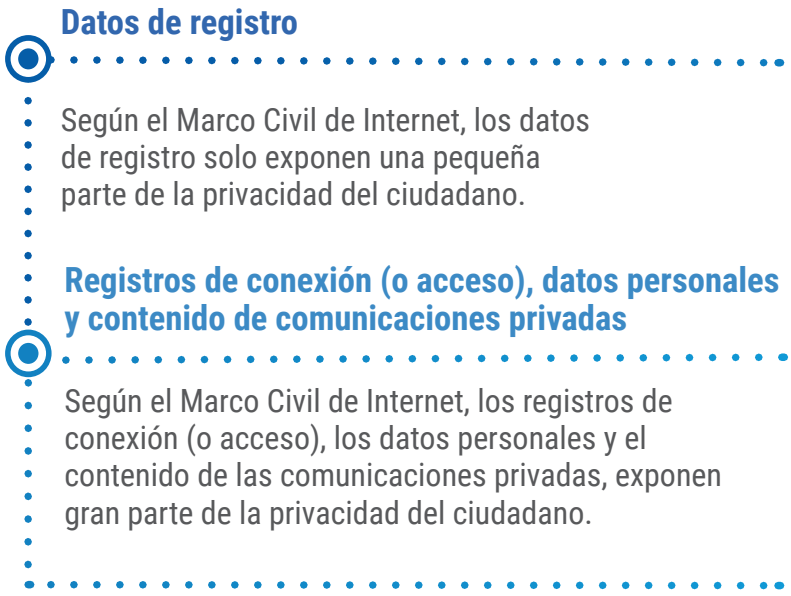


Figura 14: Categorías de los datos. **Fuente:** labSEAD-UFSC (2020).

Ahora veamos cómo el Marco Civil de Internet **protege estos registros de conexión (o acceso), datos personales y contenido de comunicaciones privadas**.

> El Marco Civil de Internet (Art. 10, § 1°) sometió la conexión (o acceso) registros, datos personales y contenido de las comunicaciones privadas a la cláusula de reserva absoluta de jurisdicción.

Esto significa que los registros de conexión y acceso a aplicaciones de *internet*, datos personales y los contenidos de las comunicaciones privadas solo pueden estar disponibles por **orden judicial**.

Además, el Marco Civil de Internet establece los requisitos que se deben cumplir para que el Poder Judicial logre otorgar una orden judicial de acceso a estos datos a la policía de investigación y el Ministerio Público. Para que estos expedientes sean solicitados, la petición de la Policía Civil, Policía Federal y el Ministerio Público deben contener tres aspectos, bajo pena de inadmisibilidad. Vamos a estudiarlos en la siguiente imagen.

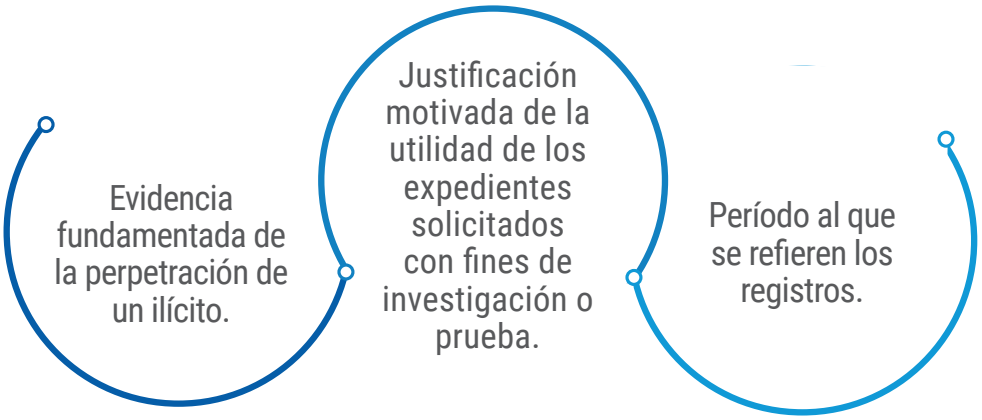


Figura 15: Aspectos para requerimento de acesso aos dados. **Fuente:** labSEAD-UFSC (2020).

Sin embargo, lo anterior no se aplica a la interceptación de **comunicaciones telemáticas**, tales como el intercambio de *e-mails* en tiempo real y el intercambio de mensajes en tiempo real - aplicaciones de mensajería, por ejemplo. En tales casos, el contenido de las comunicaciones cibernéticas privadas sólo podrá ponerse a disposición por orden judicial y, según el Marco Civil de Internet, "en la forma que la ley establezca, respetando las disposiciones de los párrafos II y III del artículo 7".

Veamos lo que establecen estas disposiciones (párrafos II y III del artículo 7).

> *Art. 7º - El acceso a internet es esencial para el ejercicio de la ciudadanía, garantizando al usuario los siguientes derechos:*
>
> *I - inviolabilidad de la intimidad y la vida privada, su protección e indemnización por los daños materiales o morales derivados de su violación;*
> *II - inviolabilidad y confidencialidad del flujo de sus comunicaciones a través de internet, salvo orden judicial, según disponga la ley. (BRASIL, 2014, traducción nuestra).*

Tengamos en cuenta que, en cuanto a las comunicaciones privadas, estas disposiciones distinguen entre las **comunicaciones que se almacenan** y el **flujo de comunicaciones**. El documento también muestra que ambas pueden ser violadas por orden judicial, pero los requisitos cambian de una modalidad a la otra.

Nótese que la redacción de los incisos II y III del artículo séptimo es prácticamente idéntica, pero en el caso de la inviolabilidad del flujo de comunicaciones, el Marco Civil menciona "en forma de ley". Por este supuesto indicado, debe entenderse que se trata de la **Ley 9.296/1996**.

> La violación de la comunicación almacenada en un dispositivo se produce con autorización judicial, pero sin requisitos legales especificados a cumplir.

En este caso, la empresa que recibe el pedido crea una **cuenta espejo**, en la cual serán reenviados los *e-mails* recibidos/enviados por el sujeto que está siendo evaluado. Obviamente, existirá un "retraso" entre el envío/recepción de mensajes por parte del destinatario y la remisión de estos datos por parte de la empresa a la cuenta espejo.

Es una cuenta paralela que recibe toda la información que llega en la cuenta principal.

En estas infracciones de comunicación almacenadas en un dispositivo, es importante solicitar la preservación del contenido a obtener, pues esto impide que los datos eliminados por el usuario dejen de estar disponibles, como veremos más adelante sobre la investigación de delitos cibernéticos.

> La violación de la comunicación de flujo se produce con autorización judicial, pero existen requisitos legales que deben cumplirse, que son los establecidos por la Ley 9.296/1996.

Otro detalle es que la mayoría de las veces el flujo de comunicaciones está encriptado, lo que genera dificultades técnicas a la hora de la intercepción. Por lo tanto, en general, los resultados tienden a ser mejores, en los casos de violación de la comunicación almacenada que en los casos de violación de la comunicación de flujo.

Saber más

Puedes acceder a la Ley 9.296/1996 completa, haciendo clic en el *link* de abajo:

http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm

Hasta ahora, hemos visto lo que Marco Civil de Internet aborda sobre los registros de conexión (o acceso), datos personales y contenido de las comunicaciones privadas.

Ahora, vamos a aprender más sobre el trato diferenciado en relación con los datos de registro.

Datos de registro

Anteriormente, observamos que el Marco Civil de Internet hace una incisión y dispensa diferentes formas de tratar datos generales y datos de registros de conexión (o acceso), datos personales y contenido de comunicaciones privadas.

En relación con los registros de conexión (o acceso), datos personales y contenido de las comunicaciones privadas, el Art. 10, § 1° del documento, los sometió a la cláusula de reserva absoluta de jurisdicción, determinando que dichos datos solo pueden ser puestos a disposición por orden judicial.

Ahora, abordaremos el trato concedido por el Marco Civil de Internet a los **datos de registro**; categoría de datos, que el enunciado extendió y que deja expuesta una pequeña porción de la privacidad del ciudadano, al compararla con la parte de privacidad que exponen los registros de conexión (o acceso), datos personales y contenido de comunicaciones privadas.

Figura 16: Datos de registro. **Fuente:** Pixabay (2020).

Con base en esta premisa, el instrumento sometió los datos de registro a la cláusula relativa de reserva de jurisdicción (Art. 10, § 3º).

> De esta forma, el acceso a los datos registrales que identifiquen calificaciones personales, filiación y domicilio, se puede hacer sin orden judicial por parte de las autoridades del Ministerio Público, Policía Civil o Policía Federal, que tengan competencia legal para su solicitud.

Es similar a la Ley de Organizaciones Criminales, que establece que el Jefe de Policía y el Ministerio Público tendrán acceso, independientemente de una autorización judicial, a los datos de registro del sujeto investigado que contengan exclusivamente su calificación personal, filiación y domicilio, datos de los que disponen los proveedores de *internet*.

Saber más

Para conocer más sobre la Ley de Organizaciones Criminales, accede al siguiente *link* y aprende más sobre lo que se aborda en relación con el tema del artículo 15 de la ley.

Ley 12.850/2013 - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

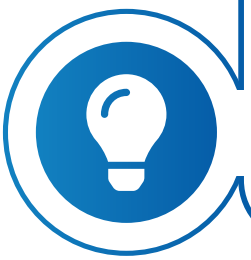
Sin embargo, a diferencia de la Ley de Organizaciones Criminales, que explica cuáles datos son considerados de registro, el Marco Civil de Internet no específica qué es el término "**datos de registro**". Por analogía, se invoca la mencionada ley, para alcanzar la comprensión del significado, de tal manera, podemos inferir que **son los datos de calificación personal, filiación y dirección, suministrada a los proveedores *internet* y a través de aplicaciones de *internet*.**

Así, según el Marco Civil de Internet, el Jefe de Policía y el Ministerio Público, sin autorización judicial, pueden solicitar datos de calificación personal, afiliación y domicilio que manejan empresas como Claro, Vivo, Tim, Net, Oi, Facebook, Instagram, Uber, etc.

Finalmente, el **Decreto 8.771/2016**, que regula el Marco Civil de Internet, establece que las autoridades administrativas indicarán la base legal con competencia expresa para el acceso y la motivación para la solicitud de dichos accesos a los datos de registro.

> Es decir, mediante este decreto, el delegado de la Policía y el Ministerio Público, al solicitar datos de registro de proveedores de conexión y proveedores de aplicaciones de *internet*, deberán citar las disposiciones jurídicas que les autorizan a presentar tal solicitud, así como deberán fundamentar y motivar la razón relativa a esa solicitud.

Finalmente, también podemos destacar que el Decreto 8.771/2016 también estipula que la Agencia Nacional de Telecomunicaciones (ANATEL) actúa en la regulación, fiscalización e investigación de infracciones relacionadas con este tema.



Saber más

Puedes acceder al texto completo del Decreto 8.771/2016 haciendo clic en el siguiente *link*:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm

Continuando con nuestros estudios, estudiemos cómo es el caso de las empresas extranjeras.

Empresas extranjeras

Si bien, por un lado, casi todos los proveedores de conexión a *internet* en Brasil (Vivo, Oi Tim, Net, Claro etc.) son empresas brasileñas, por otro lado, tenemos que la mayoría de los proveedores de aplicaciones de Internet (Facebook, WhatsApp, Yesca, Uber, etc.) son **empresas extranjeras**.

Teniendo esto en cuenta, la pregunta es: **¿las empresas extranjeras están sujetas o no a las determinaciones del Marco Civil de Internet brasileño?**

Para responder a esta pregunta, es necesario tener en cuenta que, con respecto a este tema, las empresas extranjeras se dividen en dos categorías. Vamos a conocerlas en la siguiente imagen.

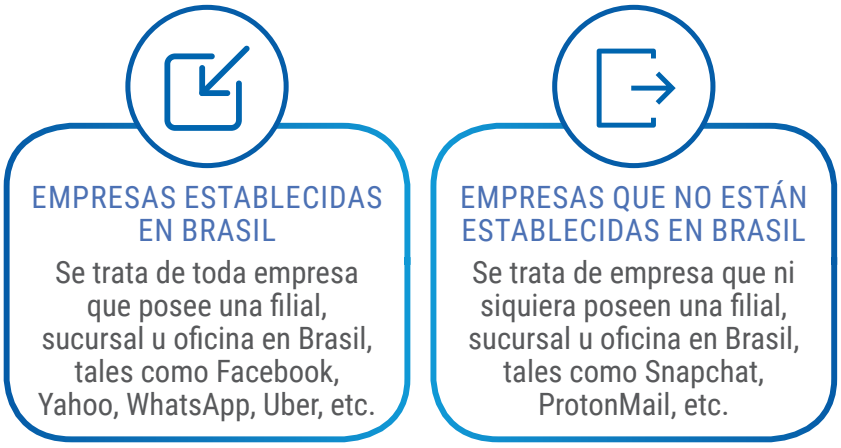


Figura 17: Categorías de las empresas extranjeras. **Fuente:** labSEAD-UFSC (2020).

Pues bien, de acuerdo con el artículo 11 del Marco Civil de Internet, incluso si tienen su sede en el extranjero, la empresa estará sujeta a cumplir con las reglas si ofrece servicios al público brasileño o si al menos un miembro de su grupo económico está establecido en Brasil; cuando se trate de una operación para recopilar, almacenar, retener y utilizar datos personales de registros o de comunicaciones, por parte de proveedores a conexión a *internet* y aplicaciones.

En este sentido, cabe señalar que el Código Civil brasileño (Ley 10.406/2002, Art. 1.126.) establece como "*nacional, la sociedad organizada de conformidad con la ley brasileña y que posea una sede administrativa en el país*". Además, el Código de Procedimiento Civil brasileño (Ley 13.105/2015, Art. 21) establece que "*se considerará domiciliada en Brasil, la entidad jurídica extranjera que posea una agencia, filial o sucursal*".

> Por lo tanto, empresas como Facebook, Yahoo!, WhatsApp, Uber etc., cuando reciben solicitudes de datos de registro por parte de delegados de Policía o del Ministerio Público, deben cumplir con la orden, bajo pena de incurrir en las sanciones establecidas por el Marco Civil de Internet, aunque son empresas extranjeras, es demostrable que ya poseen una filial o sucursal en Brasil.

Por otro lado, las empresas que no están establecidas en Brasil y ni siquiera tienen una agencia, filial o sucursal en el país, no están sujetas a las determinaciones del Marco Civil de Internet, sino a **la legislación de sus países de origen**. En tales casos las Policías Civil, Federal o el Ministerio Público deben utilizar **mecanismos de cooperación legal internacional** para obtener datos de estas empresas.

En este contexto, el artículo 12 del Marco Civil de Internet presenta cuatro tipos de sanciones administrativas para las empresas nacionales o extranjeras que incumplan las normas relativas a la custodia y disponibilidad de datos. Conócelos en la imagen a continuación.

Figura 18: Sanciones administrativas para empresas que no cumplan las normas. **Fuente:** labSEAD-UFSC (2020).

Estas sanciones que acabamos de conocer pueden ser aplicadas puntual o acumulativamente. Estas son aplicables cuando se produzcan infracciones a las normas previstas en los artículos 10 y 11 del Marco Civil, es decir, son de aplicación solo cuando existen hechos infractores, los cuales podemos identificar en la imagen a continuación.

Figura 19: Infracciones de las normas previstas en los artículos 10 y 11 del Marco Civil de Internet. **Fuente:** labSEAD-UFSC (2020).

Con relación a las infracciones, por ejemplo, si un proveedor no cumple con el orden judicial, lo que corresponde a una infracción de la legislación brasileña y, por lo tanto, es una hipótesis de aplicación de una de las sanciones previstas en el artículo 12. Y, de todas sanciones enumeradas anteriormente, vale destacar la sanción de **suspensión temporal de las actividades que involucren los actos también previstos en el artículo 11**.

Dependiendo de la violación de las normas previstas en los artículos 10 y 11 del Marco Civil de Internet, el proveedor de conexión o aplicación de *internet* podrá ser sancionado con la suspensión temporal. Dada la gravedad de esta sanción, en general, solo es decretada por el juez luego de haber decretado anteriormente sanciones más indulgentes (advertencias) y que tuvieron resultado ineficaz.

Ocurrió algunas veces, por ejemplo, con la aplicación WhatsApp.

Saiba mais

Un informe de G1 destacó los casos de suspensión de la aplicación WhatsApp por determinación de la Justicia. Verifique estos hechos accediendo al siguiente *link*.

"WhatsApp Bloqueado: Recuerda todos los casos de suspensión de la aplicación" - http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html

También podemos señalar un evento de febrero de 2015, en el que un juez de las Investigaciones Centrales del Distrito brasileño de Teresina, suspendió temporalmente WhatsApp, pues la empresa se negó a proporcionar información para una investigación policial. Como resultado, tres órdenes adicionales de suspensión de dicho servicio fueron emitidas por diferentes jueces, todas motivadas por el mismo hecho de que WhatsApp se negó a cumplir con las órdenes judiciales, incluso después de que se emitieron las advertencias y multas.

En cuanto a la **exclusión de contenidos**, el Marco Civil de Internet, en su artículo 21, establece la obligación por parte del proveedor de aplicaciones de *internet*, de eliminar el contenido generado por terceros que viole flagrantemente la intimidad de los demás, bien sean conteniéndose en ellos, escenas de desnudez o actos sexuales o cualquier otro material carácter privado, por ejemplo.

En vista de lo expuesto en relación con el Marco Civil de Internet en Brasil, podemos inferir que es el estatuto legislativo regulador del uso de Internet en el país, proporcionando principios, garantías, derechos y deberes para los que utilizan la red, así como presentando directrices e hitos para la acción de Seguridad Pública con respecto a la preservación, almacenamiento y uso de datos en los delitos cibernéticos.

Clase 3 – Crímenes Cibernéticos Previstos en la Legislación Brasileña

CONTEXTUALIZANDO...

Como ya vimos anteriormente, la legislación que rige el fenómeno de la ciberdelincuencia en Brasil es bastante reciente si se compara con las demás leyes que conforman el ordenamiento jurídico brasileño. Esto se debe a la falta de fortalecimiento de las leyes relacionadas con el crimen digital.

Así, aunque el Marco Civil de Internet reunió y consolidó las disposiciones relativas a la parte procesal del crimen digital, este instrumento no prevé crímenes. Por lo tanto, en cuanto a los crímenes electrónicos, no existe un instrumento legislativo que los agrupe, razón por lo cual, éstos se esparcen por diferentes leyes.

Entendiendo este contexto, ahora comprenderemos los delitos cibernéticos previstos en la legislación brasileña.

DELITOS CIBERNÉTICOS

Cibercrimen, crimen o delito cibernético, crimen digital, crimen o delito electrónico se entiende por **cualquier crimen practicado mediante el uso de recursos informáticos**. El **crimen cibernético** puede clasificarse en **propio** o **impropio**, como puedes ver en la siguiente imagen.

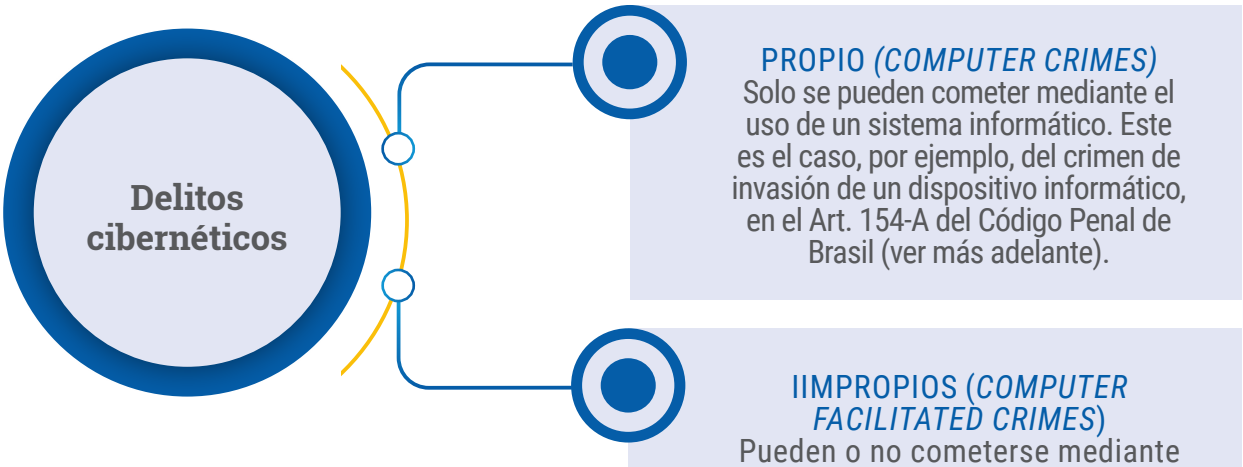


Figura 20: Clasificación de los delitos cibernéticos. **Fuente:** labSEAD-UFSC (2020).

En cuanto a los delitos cibernéticos impropios o indirectos, podemos decir que, en teoría, todos los crímenes que se constituyen como delitos cibernéticos, aunque sea de forma impropia. Incluso en caso de asesinato, como podemos ver en el siguiente ejemplo:

En la Práctica

Imaginemos la situación en la que una determinada persona es hospitalizada en terapia intensiva, con soporte vital proporcionado por dispositivos que están conectados a la red del hospital, y un hacker, con el objetivo de quitarle la vida a esta persona, invade la red del hospital y "apaga" algunos de estos dispositivos.

Debido a que, potencialmente, todo y cualquier crimen podría resultar ser un crimen cibernético impropio, es inviable comentar sobre todos los posibles tipos de delitos cibernéticos impropios.

Por esta razón, a continuación, solo discutiremos los **delitos cibernéticos propios**, previstos en la legislación brasileña.

Invasión de dispositivos informáticos

Con el advenimiento de la **Ley 12.737/2012** ("Carolina Dieckmann Law"), se creó el crimen de invasión de dispositivos informáticos. Con esta ley, se pretendía tipificar como delito la creación y difusión de virus informáticos y la invasión de sistemas (*hacking*), entre otras conductas, lo que se logró, en el artículo 154-A en el Código Penal Brasileño. En este contexto, veamos el texto de tal disposición en el **Código Penal de Brasi**l:

> *Art. 154-A — Invadir o hackear un dispositivo informático ajeno, conectado o no a la red informática, mediante la violación indebida del mecanismo de seguridad y con el fin de obtener, adulterar o destruir datos o información sin autorización expresa o tácita del titular del dispositivo, así como instalar vulnerabilidades para obtener alguna ventaja ilícita:*
>
> *Pena: detención, de tres meses a un año, y multa. (BRASIL, 2019a, traducción nuestra).*

El bien legal protegido en este caso es la privacidad, un género del cual la intimidad y la vida privada forman parte (artículo 5, letra X, de la Constitución Federal de 1988 — CF/88). Así pues, este nuevo tipo penal tutela valores constitucionalmente protegidos.

Saber más

La ley obtuvo su nombre porque la actriz Carolina Dieckman, en 2012, tenía fotos íntimas filtradas en *internet*, fotos sustraídas de su computador por *hackers*.

Puedes revisar la ley completa haciendo clic en este *link*: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Vamos a entender el **objetivo** de esta infracción. La conducta típica es "invadir". Así pues, para la configuración del delito, debe haber acceso al dispositivo electrónico necesariamente,

mediante la transposición de un mecanismo de seguridad, ya sea un ***firewall*** o una contraseña. Sin esto, el crimen no se configura.

Es un dispositivo de seguridad de red que monitorea el tráfico de la red de entrada y salida, así como también es su tarea, permitir o bloquear un tráfico sospechoso, de acuerdo con un conjunto definido de reglas de seguridad.

Entonces, por ejemplo, si una persona en el trabajo va al baño y deja su **computadora desbloqueada**, y un compañero de trabajo aprovecha el descuido, para eliminar archivos desde ese computador, **no hay ningún "hackeo"**, puesto que no existe ninguna transposición de los mecanismos de seguridad.

Asimismo, en el caso de un estafador que obtiene **acceso a una cuenta de WhatsApp** de otra persona para, a partir de ahí, realizar "estafas". **Tampoco hay delito**, ya que las cuentas de redes sociales no son exactamente "dispositivos informáticos" y porque no hubo transposición alguna de ningún mecanismo de seguridad.

Invasión de un dispositivo informático (artículo 154-A/CP de Brasil) versus robo mediante fraude (artículo 155, § 4º, II/CP de Brasil)

Imaginemos la situación en la que determinada persona invade la computadora de la víctima, instala un ***keylogger*** y captura su contraseña, ingresa a la cuenta bancaria de la víctima y le sustrae cantidades de dinero.

Keylogger - Programa informático capaz de capturar contraseñas.

¿Cuál es el crimen?

> No se trata de una invasión de un dispositivo informático, puesto que no hubo transposición alguna de un mecanismo de seguridad. Lo que se configuró fue un fraude para conseguir la contraseña de la víctima. Por tanto, el delito en este caso fue **robo mediante fraude** (artículo 155, § 4º, II/CP de Brasil).

Tengamos en cuenta que el crimen aquí constituye el **irrumpir en el dispositivo informático de otra persona mediante una violación indebida del mecanismo de seguridad para obtener datos o información**. Por tanto, este tipo de criminalidad no tipifica como delito la divulgación de la información obtenida, la cual, dependiendo de la información (si se trata de información confidencial, por ejemplo) puede configurar el **delito de divulgación del secreto**, previsto en el § 1°-A del artículo 153 del Código Penal Brasileño.

> *Art. 153 — Dar a conocer a otra persona, sin causa justa, el contenido de un documento privado o correspondencia confidencial, de quien sea destinatario o titular, y cuya divulgación pueda causar daño a terceros:*
>
> *Pena: detención, de uno a seis meses, o multa.*
>
> *§ 1° - Sólo se procede por representación.*
>
> *§ 1°- A — Dar a conocer, sin causa justa, información confidencial o sensible, según lo definido por la ley, esté o no contenida en los sistemas de información o base de datos de la Administración Pública:*
>
> *Pena: detención, de 1 (uno) a 4 (cuatro) años, y multa.*
>
> *§ 2º - B — Cuando resulten daños a la Administración Pública, la acción penal será incondicionada. (BRASIL, 2019a, traducción nuestra).*

Sería el caso, por ejemplo, de la divulgación de información confidencial en el *sitio web* Wikileaks.

El § 1° del artículo 154A del Código Penal Brasileño tipifica como crimen o delito la conducta de quienes fabriquen, ofrezcan, distribuyan o vendan a terceros, o simplemente difundan programas o dispositivos informáticos que puedan

ser utilizados por terceros para hackear otros dispositivos informáticos o instalar vulnerabilidades en ellos. Este es el caso de *troyanos* y *keylloggers*, casi siempre instalados para obtener contraseñas bancarias de los usuarios.

> *Art. 154 - A. — § 1° En la misma pena, incurren quienes producen, ofrecen, distribuyen, venden o difunden programas o dispositivos, con el fin de permitir la práctica de la conducta definida en el caput.*
>
> *§ 2º - Incrementa la pena de un sexto a un tercio si la invasión resulta en pérdidas económicas. (BRASIL, 2019a, traducción nuestra).*

En este contexto, aunque menciona programas o dispositivos de computación, esto incluye un *hardware* destinado a la invasión de dispositivos informáticos. En el segundo párrafo, se prevé un aumento de la pena de 1/6 a 1/3 en caso de una pérdida económica derivada de la realización de dicha invasión de un dispositivo informático. Además, la pena se incrementa de 1/3 a 1/2 si el delito se comete contra determinadas autoridades.

Veamos, en la siguiente imagen, cuáles son esas autoridades señaladas.

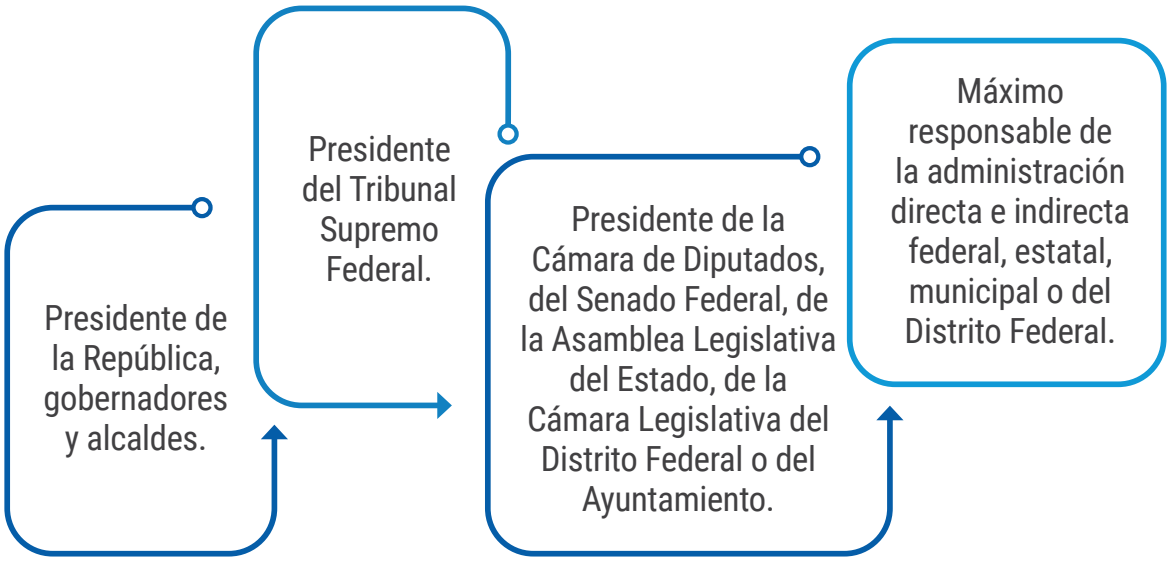


Figura 21: La pena por un delito aumenta si se comete contra determinadas autoridades, según el § 5º del artículo 154-A del CP. **Fuente:** labSEAD-UFSC (2020).

El Código Penal también dispone, en el § 3º del artículo 154-A, que habrá un calificativo si, con la invasión, el agente consigue obtener algún contenido específico. Conócelos en la imagen de abajo.

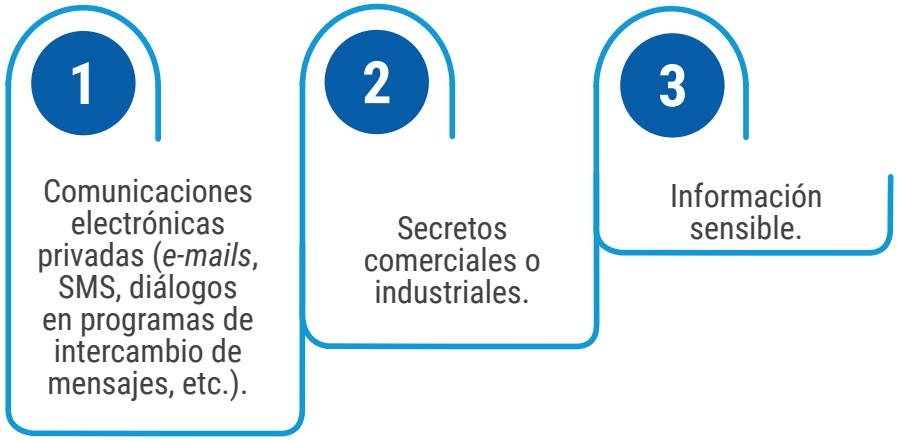


Figura 22: Datos obtenidos por la invasión que califican al crimen. **Fuente:** labSEAD-UFSC (2020).

Veamos lo que dice el Código Penal de Brasil en el tercer párrafo del artículo 154-A:

> *Si la invasión resulta en la obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, información sigilosa, según lo defina la ley, o mediante el control remoto no autorizado del dispositivo invadido:*
>
> *Pena: prisión de seis meses a dos años, y multa si la conducta no configura un delito más grave. (BRASIL, 2019a, traducción nuestra).*

En cuanto a este párrafo, cabe señalar que este crimen no debe confundirse con el crimen tipificado en el artículo 10 de la Ley 9.296/1996. Si el acceso a comunicaciones electrónicas privadas (*e-mails*, SMS, diálogos en programas de intercambio de mensajes, etc.) **ocurre cuando éstas se encuentran almacenadas en un computador**, se trata del crimen del artículo 154-A. Por otro lado, si **se interceptan las comunicaciones electrónicas privadas**, se incurrirá en la infracción del artículo 10 de la **Ley 9.296/1996** (la cual estudiaremos con mayor detalle, más adelante).

En los casos de forma calificada, la sanción se incrementa de 1/3 a 2/3 si hay **divulgación, comercialización o traspaso a terceros, en cualquier título**, de los datos o información obtenida. Es un **crimen doloso**. Este tipo penal, requiere de la presencia de una finalidad especial para actuar y, por tanto, solo se configura si la invasión se produce con dos objetivos, presentados en la imagen a continuación.

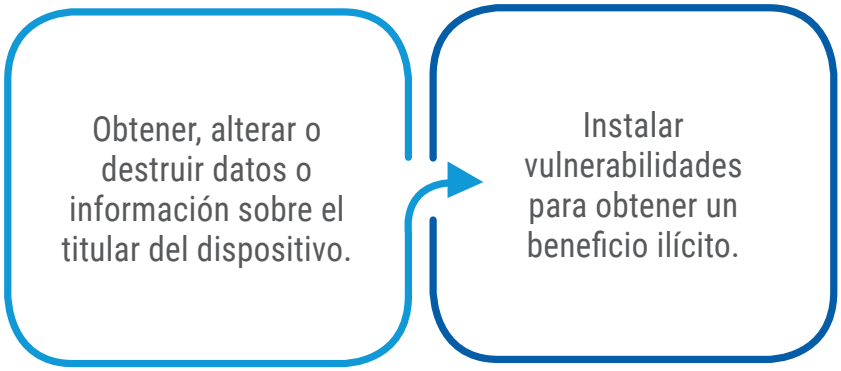


Figura 23: Configuración de la invasión como crimen. **Fuente:** labSEAD-UFSC (2020).

El crimen es formal, es decir, **se configura con la invasión**, no requiriendo el acontecimiento de las consecuencias naturales, de este tipo de ilícitos. De esa forma, la mera obtención, manipulación o destrucción efectiva de datos sobre el titular del dispositivo o la instalación de vulnerabilidades, no necesita producir efectos para que el delito sea consumado.

Por regla general, para probar la invasión es necesario realizar una investigación pericial, de acuerdo con el Artículo 158 del Código Procesal Penal de Brasil (CPP). Sin embargo, es posible que el delito sea probado por otros medios, como la prueba testimonial, por ejemplo (artículo 167 del CPP brasileño).

Con relación a **la acción penal**, el crimen del artículo 154-A, por regla general, es de **acción penal pública sujeta a representación,** es decir, es necesario el **consentimiento de la víctima** para que el Estado investigue, procese y juzgue ese caso. Esto se explica porque se trata de un crimen o delito que involucra intimidad y la vida privada, por lo que la investigación, el enjuiciamiento y la sentencia del crimen, puede resultar traumáticas para la víctima.

Excepcionalmente, el delito del artículo 154-A será una acción pública incondicional si se comete contra dos ramas. Identifiquémoslos en la imagen de abajo.

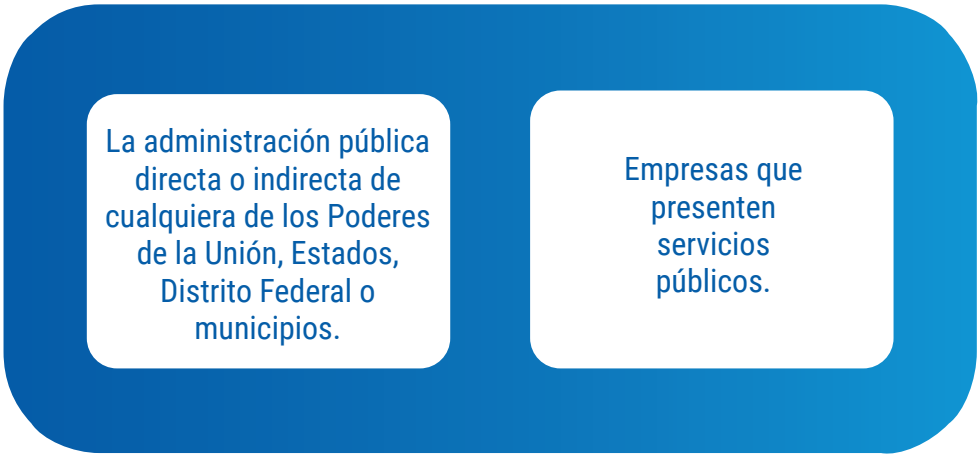


Figura 24: Ramas que, al ser atacadas, caracterizan un delito de acción pública incondicionada. **Fuente:** labSEAD-UFSC (2020).

Finalmente, entendemos que en los delitos tipificados en el artículo 154-A sólo se procede por representación, salvo que el delito se cometa contra la administración pública directa o indirecta de alguno de los Poderes de la Unión, los estados, el Distrito Federal o los municipios o contra empresas de servicios públicos.

Crimen de interceptación ilícita de comunicaciones (artículo 10 de la Ley 9.296/1996)

Cuando iniciamos el estudio del crimen de Invasión de Dispositivo Informático, observamos que éste no debe confundirse con el crimen previsto en el § 3º del artículo 154-A con el crimen del artículo 10 de la Ley 9.296/1996, que trata de la interceptación ilícita de comunicaciones telemáticas.

Estudiar lo tipificado en el artículo 10 de la Ley 9.296/1996.

> *Es delito interceptar comunicaciones telefónicas, informáticas o telemáticas, o quebrantar secretos de los tribunales, sin autorización judicial o con fines no autorizados por la ley.*
>
> *Pena: prisión de dos a cuatro años y multa. (BRASIL, 1996, traducción nuestra).*

De la lectura de tal disposición, parece que hay dos conductas incriminatorias en este artículo. Analicémoslas en la siguiente imagen.

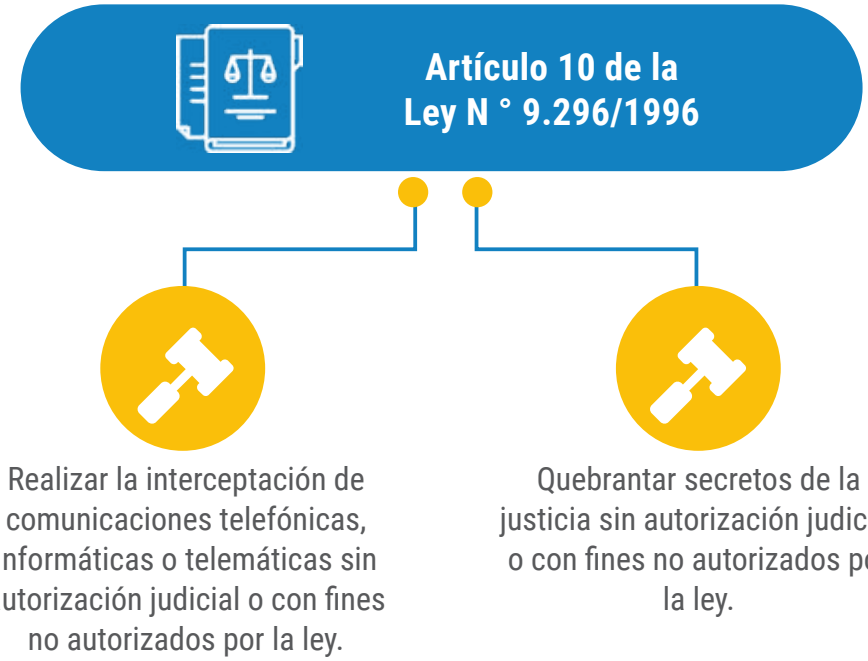


Figura 25: Conductas incriminatorias en el artículo 10 de Ley 9.296/1996. **Fuente:** labSEAD-UFSC (2020).

Sin embargo, la Ley 9.296/1996 establece que sus disposiciones pueden aplicarse a la interceptación de datos. En otras palabras, esta ley también sirve para interceptar el flujo de datos entre dos computadoras, como *e-mails*, *chats*, comunicaciones instantáneas, etc.

Así, podemos concluir que si por un lado, la invasión de un dispositivo informático seguida del acceso a comunicaciones electrónicas privadas (*e-mails*, SMS, diálogos en programas de intercambio, etc.) almacenadas en un ordenador configura el delito del artículo 154-A, por otro lado, la interceptación de comunicaciones electrónicas privadas configura el artículo 10 de la Ley 9.296/1996.

Saber más

Para mejorar tus conocimientos, puedes acceder a la Ley 9.296/1996 completa haciendo clic en este *link*: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm

Continuando los estudios, conoceremos el crimen de introducir datos falsos en sistemas de información y también la modificación o alteración no autorizada de sistemas de información. ¡Adelante!

Crimen de insertar datos falsos en el sistema de información y modificación o alteración no autorizada del sistema de información

Crimen de insertar datos falsos en el sistema de información

Otro delito que podemos destacar y que está presente en la legislación brasileña es la inserción de datos falsos en sistemas de información. Para comprender bien, ejemplificamos con un caso de finales de 2019 en el que la prensa informó que el Departamento de Tránsito del Distrito Federal (DENTRAN) investigó la supuesta práctica irregular de cancelar multas dentro de la agencia. Otro ejemplo es la alteración ilícita de bases de datos públicas, que es un fenómeno común y, durante mucho tiempo, ha sido considerado un delito en Brasil.

Saber más

Para ilustrar el crimen con más claridad, señalaremos un caso registrado en 2019. Conócelo haciendo clic en el *link* a continuación.

"DF: DETRAN investiga cancelamiento indebido de multas por agentes" - https://www.metropoles.com/distrito-federal/df-detran-investiga-cancelamento-indevido-de-multas-por-agentes

En el año 2000, la **Ley 9.983/2000** incluyó, entre otros crímenes, en el Código Penal, el crimen de "**Ingresar datos falsos en el sistema de informaciones**" y el de "**Modificación o alteración no autorizada del sistema de informaciones**". En este sentido, veamos a continuación lo que establece el artículo 313-A del CP brasileño:

> *Insertar o facilitar, al funcionario autorizado, el ingreso de datos falsos, alterar o eliminar indebidamente datos correctos en los sistemas informáticos o bases de datos de la Administración Pública con el fin de obtener un beneficio indebido para sí mismo, para los demás o para causar daño a terceros:*
>
> *Pena - prisión, de dos a doce años, y multa. (BRASIL, 2019a, traducción nuestra).*

La conducta típica de este delito, apodada por los autores del derecho penal como "malversación electrónica", consiste en obtener beneficios indebidos para sí mismo o para causar daño a terceros, como podemos ver a continuación.

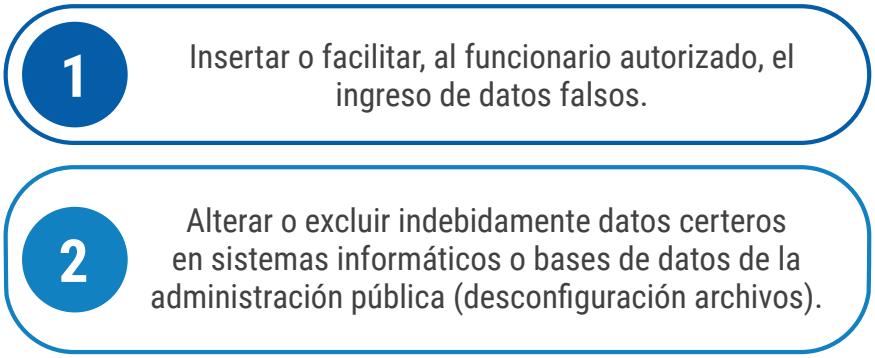
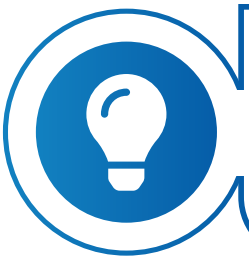


Figura 26: Conducta típica del crimen de insertar datos falsos en un sistema de información. **Fuente:** labSEAD-UFSC (2020).

Con respecto a este delito, cabe señalar que se trata de **delito propio** que sólo puede ser cometido por el funcionario público autorizado a introducir datos electrónicos. Procedamos ahora, al estudio del delito de modificación o modificación no autorizada del sistema de información.



Saber más

Para mejorar tus conocimientos, puedes conocer con la Ley 9.983/2000 completa haciendo clic en el *link*: http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm

Ahora, comencemos el estudio sobre el crimen de modificación o alteración no autorizada del sistema de información.

Crimen de modificación o alteración no autorizadas del sistema de información

Junto con el delito de insertar datos falsos en el sistema de información y otros, la Ley 9.983/2000 incluyó, en el Código Penal Brasileño, el crimen o delito de **modificación o alteración no autorizada del sistema de información**.

El artículo 313-B del Código Penal de Brasil, que tipifica este delito es el siguiente:

> *Modificar o modificar el oficial, el sistema de información o el programa informático sin autorización o solicitud de la autoridad competente:*
>
> *Pena: prisión, de tres meses a dos años, y multa.*
> *Párrafo único. Las sanciones se incrementan de un tercio a la mitad si la modificación o alteración ocasiona daños a la Administración Pública o a la Administración. (BRASIL, 2019a, traducción nuestra).*

La conducta típica, en este caso, es que el funcionario modifique o altere el sistema de información o software sin autorización o solicitud de la autoridad competente. Nótese que el delito de insertar datos falsos en el sistema de información, previsto en el artículo 313-A del Código Penal de Brasil, se refiere a datos provenientes de sistemas electrónicos,

mientras que aquí se relaciona el delito de modificación o alteración no autorizada del sistema de información, modificaciones/alteraciones del propio sistema electrónico.

Nuevamente, además de lo comentado con relación al delito en el artículo 313-A, el delito de modificación o alteración no autorizada del sistema de información es **delito propio**, ya que solo el funcionario público puede practicarlo.

En el caso de esta infracción, las penas se incrementan de 1/3 a 1/2 si la modificación o alteración da como resultado un daño a la administración pública o al administrador.

Finalmente, cabe señalar que el delito de insertar datos falsos en el sistema de información no prevé un aumento de la pena de un tercio a la mitad, si la acción da lugar a un perjuicio para la administración pública o el administrador. Dicha disposición se encuentra únicamente en el único párrafo del artículo 313-B, que trata de la modificación o alteración no autorizada del sistema de información.

Crimen de interrupción o perturbación del servicio telegráfico, telefónico, informático, telemático o de información de utilidad pública

El crimen de interrupción o alteración de los servicios telegráficos, telefónicos, informáticos, telemáticos o de información de utilidad pública, previsto en el artículo 266 del Código Penal Brasileño, comprende las conductas que afecten a diversos servicios. Por lo tanto, con respecto al ataque a estos servicios, el delito previsto es un **crimen cibernético propio**.

Veamos lo que establece en sus disposiciones:

> *Artículo 266 - Interrumpir o perturbar el servicio telegráfico, radiotelegráfico o telefónico, impidiendo o entorpeciendo su restablecimiento:*
>
> *Pena - prisión de uno a tres años y multa.*
>
> *§ 1° Incurre la misma pena quien interrumpa un servicio telemático o de información de utilidad pública, o impida o dificulte el restablecimiento de la misma sanción.*
>
> *§ 2º Se aplican penas dobles si el delito se comete para ocasionar una calamidad pública. (BRASIL, 2019a, traducción nuestra).*

Las dos opciones a continuación se consideran crimen aquí. ¡Analízalas!

Interrumpir o perturbar los servicios telegráficos, telefónicos, informáticos, telemáticos o de información de utilidad pública.

Impedir u obstaculizar la restauración de estos servicios cuando hayan sido interrumpidos.

Figura 27: Conducta típica del delito de interrupción o perturbación de servicios telegráficos, telefónicos, informáticos, telemáticos o de información de utilidad pública. **Fuente:** labSEAD-UFSC (2020).

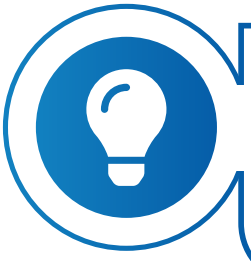
Un ejemplo de estos crímenes es el "**ataques de denegación de servicio**" (también conocidos como DDoS, un acrónimo en inglés para Distributed Denial of Service). Por regla general, estos ataques consisten en un intento de hacer que los recursos del sistema no estén disponibles para sus usuarios a través de su invalidación por sobrecarga. Esto se hace mediante el envío de múltiples solicitudes al servicio para que sea "sobrecargado", de modo que este servicio no soporte el exceso de demanda y "se detenga". En 2011, por ejemplo, un ataque *hackers* derribó los *sitios web* de la Presidencia de la República, de la Receita Federal de Brasil y del Portal Brasil.

Este crimen se consuma con la práctica de la conducta descrita, y no hay necesidad de daño o consecuencias para la configuración del ilícito. Es decir, **el mero "ataque de denegación de servicio", incluso si no "derriba" el *sitio web*, consuma el crimen** (es decir, se trata de un crimen de **peligro abstracto** o **presumible**).

En otro enfoque relacionado con este crimen dentro de la legislación, podemos observar que la protección de los servicios informáticos, telemáticos o la información de utilidad pública se incluyen en la figura de equivalente del crimen en el § 1°. Veamos.

> *Artículo 266 - Interrumpir o perturbar el servicio telegráfico, radiotelegráfico o telefónico, impidiendo o dificultando su restablecimiento:*
>
> *Pena - detención, de uno a tres años, y multa.*
>
> *§ 1° Incurre en la misma pena quien interrumpa un servicio telemático o de información de utilidad pública, impida o dificulte el restablecimiento de la misma sanción. (BRASIL, 2019a, traducción nuestra).*

Los párrafos primero y segundo fueron insertados allí por la **Ley 12.737, de 2012** y, antes, el delito mencionaba únicamente los servicios telefónicos, telegráficos, radiotelegráficos, estos dos últimos prácticamente inexistentes en la actualidad. Finalmente, podemos resaltar que se aplican dobles penas si el delito se comete en caso de calamidad pública.



Saber más

Conoce la Ley 12.737/2012 en su totalidad haciendo clic en el siguiente *link*: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Aún analizando la legislación brasileña con relación a los crímenes digitales, podemos evidenciar que otras leyes caracterizan tipologías de este delito.

¡Sigamos aprendiendo más!

CRÍMENES DE VIOLACIÓN DE DERECHOS DE AUTOR DE PROGRAMAS INFORMÁTICOS

Con el objetivo de aprender sobre el crimen **de violación de derechos de autor del programa informático**, tenemos que comenzar por la Ley de Software. En este sentido, la Constitución Federal confiere una protección especial a la propiedad intelectual.

Veamos en la siguiente imagen, lo que cubre en su quinto artículo.

1

XXVII – Los autores tienen el derecho exclusivo de utilizar, publicar o reproducir sus obras, transferible a sus herederos durante el tiempo que establezca la ley.

2

XXVIII – Según la ley, se garantiza lo siguiente:

a. la protección de la participación individual en obras colectivas y la reproducción de la imagen y voz humana, incluidas en las actividades deportivas.

b. el derecho a fiscalizar el uso económico de las obras que crearon o en las que participen los creadores, intérpretes, y las respectivas representaciones gremiales.

3

XXIX – La ley otorgará a los autores de invenciones industriales, privilegio temporal para su uso, así como protección a las creaciones industriales, titularidad de marcas, nombres de empresas y otros signos distintivos, con miras al interés social y al desarrollo tecnológico, y económico del país.

Figura 28: Art. 5 de la Constitución Federal.
Fuente: labSEAD-UFSC (2020).

Así, para otorgar legítima protección a la propiedad intelectual de los programas informáticos, se promulgó la **Ley 9.609/1998, Ley de Software.** Esta ley otorga a la propiedad intelectual de los programas informáticos el mismo régimen que se le da a las obras literarias bajo el derecho de autor y legislación relacionada vigente en el país.

> Esta protección y tutela de los derechos sobre los programas informáticos se concede por un período de 50 años, a partir del 1 de enero del año siguiente a su publicación o, en su defecto, a su creación.

Veamos lo que establece el segundo artículo de la Ley 9.609/1998.

> *El régimen de protección de la propiedad intelectual de un programa informático es el conferido a las obras literarias la legislación de derecho de autor y afines vigente en el país, con sujeción a lo dispuesto en esta Ley.*
> *[...]*

§ 2º La tutela de derechos relacionados con un programa informático se otorga por un período de 50 años, a contar desde el 1 de enero del año siguiente a su publicación o, en su defecto, de su creación. (BRASIL, 1998, traducción nuestra).

Con el fin de brindar protección a la propiedad intelectual de un programa informático, la Ley 9.609/1998 prevé, en su artículo 12, el **crimen de violación de los derechos de autor de programas informáticos**.

Saber más

Para mejorar tus conocimientos, puedes ingresar al *link* a continuación y leer la Ley 9.609/1998 completa:

http://www.planalto.gov.br/ccivil_03/leis/L9609.htm

Ahora, vamos a continuar con nuestro estudio sobre la Ley de Software, que prevé el crimen de violación de los derechos de autor de programas informáticos, conociendo más sobre el artículo 12 de la ley antes mencionada.

El crimen de violación de los derechos de autor de programas informáticos está tipificado en el artículo 12 de la Ley 9.609/1998. Veamos lo que establece el artículo:

Artículo 12 - Violación de los derechos de autor de programa informáticos:

Pena - prisión de seis meses a dos años o multa.

§ 1° Si la infracción consiste en la reproducción, por cualquier medio, de un programa informático, total o parcial, con fines comerciales, sin la autorización expresa del autor o de quien lo represente:

Pena - prisión de uno a cuatro años y multa.

> *§ 2º Incurre en la misma pena que en el párrafo anterior, quien incurre el que venda, exponga para la venta, introduzca en el país, adquiera, esconda o almacene, con fines comerciales, un original o copia de un programa informático, configurando así la violación de los derechos de autor. (BRASIL, 1998, traducción nuestra).*

O El crimen, en este caso, consiste en violar los derechos de autor del programa informático. Se trata de un crimen especial en relación con el crimen o delito de violación de derechos de autor previsto en el artículo 184 del Código Penal de Brasil.

De igual manera, observemos que el § 2º menciona el término "introduce al país", lo que implica que cuando se introduce al país un *software* producido bajo violación de los derechos de autor, según el principio de especialidad, no caberá el ilícito de contrabando ni malversación, pero sí, el crimen del artículo 12 de la Ley 9.609/1998.

En cuanto a la penalización de estas conductas, el legislador planteó hipótesis en las que determinadas conductas no constituyen vulneración de los derechos del titular del programa informático. Por tanto, algunos aspectos no vulneran los derechos del propietario del programa informático.

Vamos a identificarlos en la siguiente imagen.

La reproducción, en un solo tenor, de una copia legítimamente adquirida, siempre esta copia sea destinada para la preservación o almacenamiento electrónico de la misma, en cuyo caso la copia original servirá de salvaguardo.

Citación parcial del programa, con fines didácticos, siempre que se identifique el programa y el titular de los derechos respectivos.

La aparición de semejanza de un programa con otro, preexistente, cuando se configura por las características funcionales de su aplicación, la observancia de preceptos normativos y técnicos semejantes, o de limitación de forma alternativa para su expresión.

La integración de un programa, manteniendo sus características esenciales, a una aplicación o sistema operativo, técnicamente indispensable a las necesidades del usuario, siempre que sea para uso exclusivo de quienes lo promocionan.

Figura 29: Conductas de los delitos, en el artículo sexto de la Ley 9.609/1998.
Fuente: labSEAD-UFSC (2020).

Ahora que sabemos más sobre este crimen, continuemos con nuestro contenido y recorramos el concepto del principio de adecuación social.

Principio de adecuación social

La piratería siempre ha sido un delito recurrente en Brasil. En este contexto, algunos tribunales aplicaron el **principio de adecuación social** para excluir la tipicidad de la conducta de exponer a la venta CD y DVD pirateados.

Por ejemplo, en el juicio de Apelación Especial 1.193.196, un caso de repercusión en el estado de Minas Gerais, el Tribunal Superior de Justicia (STJ) se evaluó la conducta de una mujer que mantenía en sus locales comerciales, la exposición a la venta de 170 DVDs y 172 CDs “piratas”. El juez de primer grado, al aplicar el principio de adecuación social, decantó por la absolución y la justicia estatal mantuvo dicha resolución atípica. **Sin embargo, el STJ entendió que la adecuación social no se aplica a este caso y editó el Resumen 502**. Veamos lo que dice este Resumen.

> *Con respecto a la materialidad y la autoría, parece típico, en relación con el delito previsto en el artículo 184, párrafo 2 del Código Penal, la conducta de exponer a la venta CD piratas y DVD. (BRASIL, 2012).*

Dentro de este principio, tenemos la **forma calificada del delito**, si la violación consiste en la reproducción, por cualquier medio, de un programa informático, total o parcialmente, para el fines comerciales, sin el permiso expreso del autor o de la persona que lo representa (la autorización, es una conducta es atípica).

> También se califica cuando aquellos que venden, exponen para la venta, introducen en el país, adquieren, ocultan o mantienen en depósitos, para fines comerciales, un original o copia de algún programa informático, producido bajo violación de derechos de autor.

Los programas de **computador reproducidos ilegalmente**, cuando se venden o distribuyen, configuran, en relación con **quienes los reciben/compran**, el delito de **receptación** (artículo 180 del Código Penal Brasileño), puesto que esas copias reproducidas sin la autorización expresa del autor, o de la persona que lo representa, constituyen el producto del crimen o delito.

En cuanto a la acción penal accionable sobre **el crimen**, conforme a lo previsto en el párrafo 3º del artículo 12 de la Ley 9.609/1998, la acción penal será de **dominio privado**. No obstante, según lo previsto en los incisos I y II del § 3º del mismo artículo de la misma ley, que podemos observar en la siguiente imagen, en cuáles crímenes específicos la acción penal será pública.

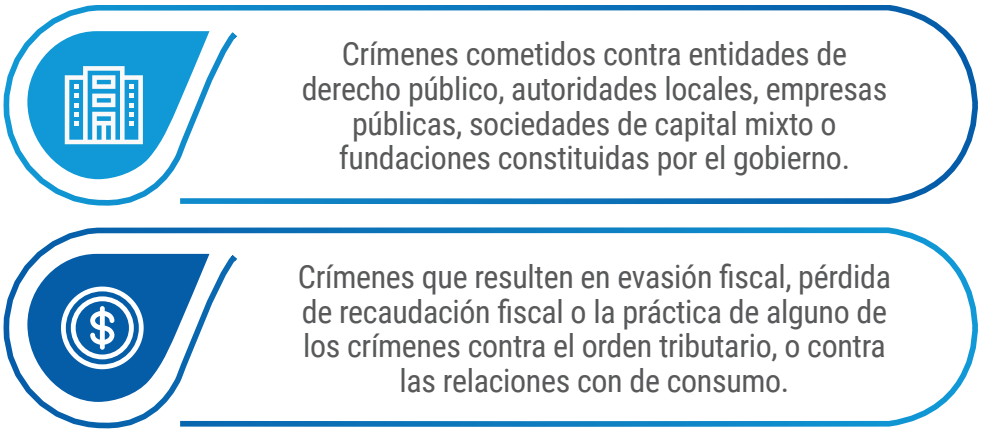


Figura 30: Párrafo tercero del artículo 12 de la Ley 9.609/1998.
Fuente: labSEAD-UFSC (2020).

Por lo tanto, entendemos el principio de adecuación social relacionado con los delitos de piratería en el país.

Continuemos nuestros estudios y aprendamos sobre otro crimen digital previsto en la legislación brasileña.

Crimen del Estatuto de la Niñez y la Adolescencia

O El artículo 241-A del Estatuto de la Niñez y la Adolescencia (ECA) — **Ley 8.069, de 13 de julio de 1990** — presenta un **propio delito cibernético**, que es el **delito de manipulación de material pornográfico infantil a través de un sistema informático o telemático**.

Veamos lo que establece dicha disposición:

> *Art. 241-A - Ofrecer, intercambiar, poner a disposición, transmitir, distribuir, publicar o difundir por cualquier medio, incluso por medio de un sistema informático o telemático, una fotografía, video u otro registro que contenga una escena sexual explícita o pornográfica que involucre a un niño o adolescente:*
>
> *Pena - prisión, de tres a seis años y multa.*
>
> *§ 1º Incurrirán en la misma pena quienes:*

I - proporcione, por cualquier medio, el acceso a la red informática a fotografías, escenas o imágenes, a las que se refiere el caput de este artículo.
II - garantizar, por cualquier medio, el acceso por red informática a las fotografías, escenas o imágenes a las que se refiere el título de este artículo.

§ 2º Las conductas tipificadas en los incisos I y II del § 1º de este artículo son punibles cuando el responsable legal de la prestación del servicio, oficialmente notificado, deje de inhabilitar el acceso a dichos contenidos ilícitos a los que se refiere el capítulo de este artículo. (BRASIL, 2019c).

La expresión "**escena sexual explícita o pornográfica"** incluye cualquier situación que involucre a un niño o adolescente en actividades sexuales explícitas, reales o simuladas, o la exhibición de genitales o adolescentes de un niño con fines primordialmente sexuales, como se explica en el artículo 241-E.

Saber más

Para acceder al material completo de la Ley 8.069 de 13 de julio de 1990, puedes hacer clic en el siguiente *link*:

Estatuto de la Niñez y la Adolescencia (ECA en portugués) – http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

Más allá del crimen de *caput* del artículo 241a, el instrumento contempla conductas equivalentes a este delito en el primer párrafo. Veamos, en la imagen a continuación, e identifiquemos cuáles prácticas destacan a quién comete el delito.

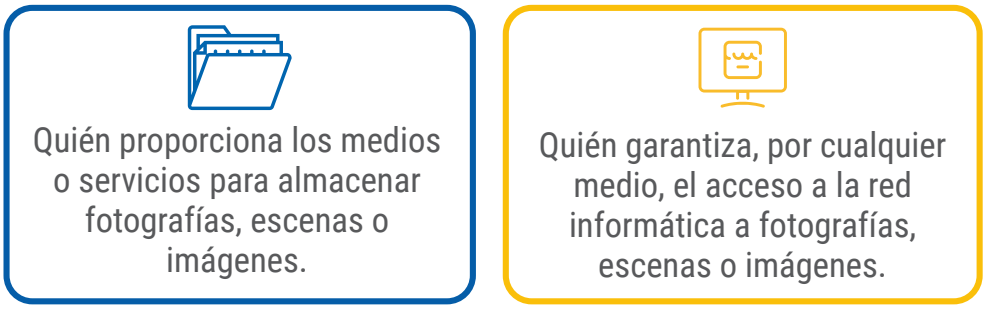


Figura 31: Acciones penales en relación con el delito iniciadas por la ECA. **Fuente:** labSEAD-UFSC (2020).

En el contexto del crimen del Art. 241-A del Estatuto del Niño y del Adolescente (ECA en portugués), es importante señalar que una persona que almacena en su computadora videos pornográficos que involucran a niños, niñas y adolescentes, aunque no comete el delito del artículo 241-A, comete otro delito, que es delito del artículo 241-B del ECA.

Veamos lo que establece esta disposición:

> *Art. 241-B - Adquirir, poseer o almacenar, por cualquier medio, una fotografía, video u otra forma de registro que contenga una escena explícita sexual o pornográfica que involucre a un niño o adolescente:*
>
> *Pena - prisión, de uno a cuatro años y multa.*
>
> *§ 1° La pena se reduce a uno de los tercios si el material al que se refiere el caput de este artículo es pequeño.*
>
> *§ 2º No se configura el crimen, en el caso que el almacenamiento de ese material tenga como finalidad comunicar a las autoridades competentes del suceso de la conducta descrita en los artículos 240, 241, 241-A y 241-C de esta Ley, siempre y cuando la comunicación se haga a través de:*
>
> *I - un agente público en el ejercicio de sus funciones;*
> *II - un miembro de una entidad legalmente constituida que incluya, entre sus fines institucionales, la recepción, procesamiento y transmisión de noticias que involucren los crímenes a que se refiere este parágrafo;*
> *III - representante legal y funcionarios responsables de un proveedor de acceso o servicio prestado a través de una red informática, hasta la recepción del material relacionado con el ilícito a la autoridad policial, al Ministerio Público o al Poder Judicial.*

> *§ 3º Las personas a que se refiere el § 2º de este artículo deberán mantener la confidencialidad del material ilícito referido. (BRASIL, 2019c, traducción nuestra).*

Es decir, el crimen consiste en adquirir, poseer o almacenar, por cualquier medio, una fotografía, vídeo u otra forma de registro que contenga escenas sexuales explícitas o pornográficas en las que participen niños, niñas y adolescentes. Se observa que la sanción se reduce de uno a dos tercios si la cantidad del material mencionado en el *caput* de este artículo es pequeña.

Además, no existe delito si la posesión o almacenamiento tiene por objeto informar a las autoridades competentes de la conducta descrita en los artículos 240, 241, 241-A y 241-C del ECA. Sin embargo, este supuesto sólo es válido cuando la comunicación fue hecha ante personas responsables.

Identifica aquellas personas responsables en la imagen a continuación.

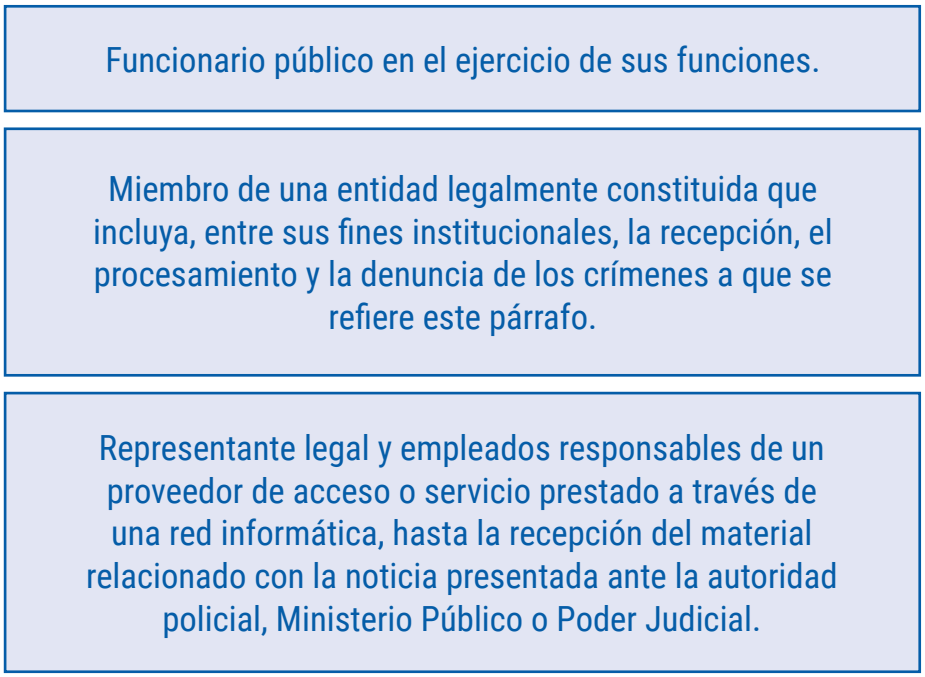


Figura 32: Personas responsables del almacenamiento de datos que caracterizan este delito y sus particularidades. **Fuente:** labSEAD-UFSC (2020).

Este delito es un delito muy común e intensamente reprimido en la forma que es calificado por la Policía Civil. En este sentido, por ejemplo, cabe destacar la Operação Luz na

Infância, un operativo policial periódico en el que el Ministerio de Justicia y la Policía Civil de los estados, unieron fuerzas reprimiendo e investigando los delitos de abuso y explotación sexual contra niños, niñas y adolescentes llevados a cabo en *internet*, especialmente los delitos de almacenar, compartir y producir pornografía infantil.

Aunque el alcance de la operación es más amplio, casi todas las situaciones de detención en flagrancia, detectados en medio las actuaciones de la Operación Luz na Infância se relacionan con el delito de almacenamiento de pornografía infantil, es decir, explícitamente el delito del Art. 241-B.

Crimen del artículo 218-C del Código Penal Brasileño

El artículo 218-C del Código Penal tipifica el delito de revelar la escena de una violación o la escena de una violación de una persona vulnerable, una escena de sexo o pornografía:

> *Art. 218-C - Ofrecer, intercambiar, poner a disposición, transmitir, vender o exhibir para la venta, distribución, publicación o divulgación, por cualquier medio, incluso a través de comunicación masiva o sistema informático o telemático, una fotografía, video u otro registro audiovisual que contenga escenas de violación o violación de vulnerables.*
>
> *Pena - reclusión de uno a cinco años, si el hecho no constituye un delito más grave.*
>
> **Aumento de la pena**
>
> *§ 1° - La pena se incrementa de un tercio a dos tercios si el delito es cometido por un agente que mantiene o ha mantenido una relación íntima o de afecto con la víctima con el fin de venganza o humillación.*

Exclusión de la ilegalidad

> *§ 2º - No hay delito cuando el agente practica las conductas descrita en el caput de este artículo en publicaciones periodísticas, científicas, culturales o académicas con la -imprescindible- adopción de un recurso que imposibilite la identificación de la víctima, salvo autorización previa, si la víctima es mayor de 18 (dieciocho) años. (BRASIL, 2019a, traducción nuestra).*

En efecto, el artículo 218-C del Código Penal contiene en realidad dos grupos distintos de conducta. Vamos a conocer estos grupos analizando la siguiente imagen:

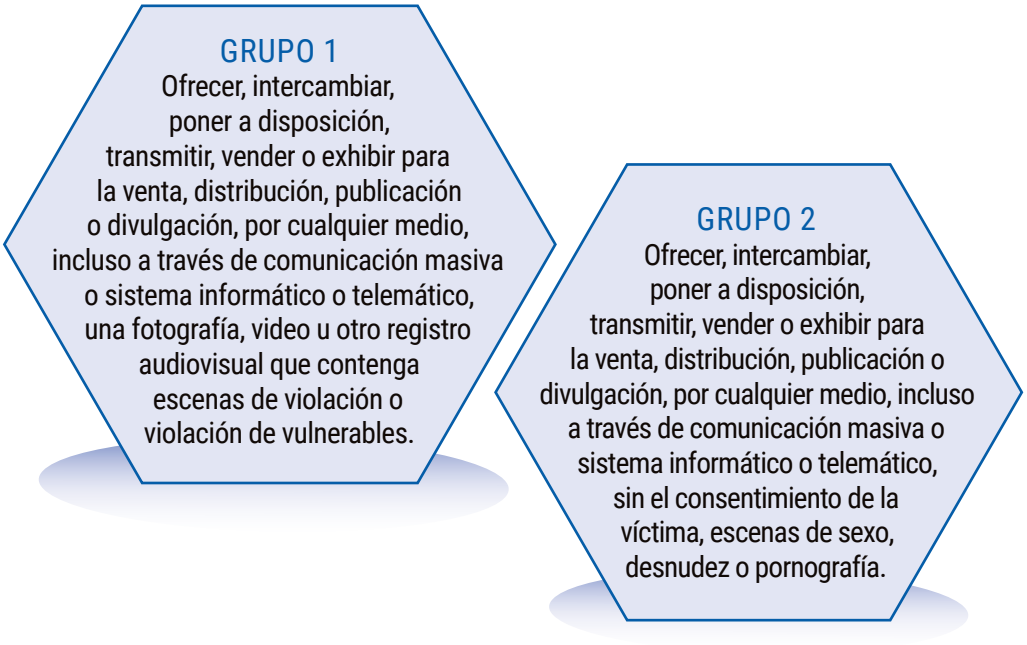


Figura 33: Diferentes grupos de conductas relacionadas con el delito tipificado en el artículo 218-C del Código Penal. **Fuente:** labSEAD-UFSC (2020).

Así, el crimen o delito se configura tanto si las conductas implican "fotografía, vídeo u otro registro audiovisual que contenga escenas de violación o violación de vulnerables [...]" o si se trata de escenas "[...] sin el consentimiento de la víctima, escenas sexuales, de desnudez o pornografía". (BRASIL, 2019a, traducción nuestra).

Cabe señalar que, a diferencia del delito de "adquirir, poseer o almacenar fotografías o vídeos que contengan escenas sexuales explícitas o pornográficas en las que participen

niños, niñas y adolescentes" (previsto en el artículo 241-B del Estatuto de la Niñez y la Adolescencia), la posesión de este tipo de material no ha sido tipificada como delito en este caso. Por tanto, no configura un crimen tener, por ejemplo, fotografías o videos de este tipo en tu teléfono celular (a menos que el material refiera a niños, niñas o adolescentes).

> Otro detalle es que cualquier persona puede ser víctima de este delito (la víctima, en este caso, es la persona que forma parte de la fotografía o video), pero hay que prestar atención al hecho de que, si es menor, no será el delito del artículo 218-C del CP de Brasil, pero sí delito del artículo 241-A del ECA.

La pena se incrementará de un tercio a dos tercios si:

- El crimen lo practica un agente que mantiene o ha mantenido una relación íntima o de afecto con la víctima.
- El crimen se practica con el propósito de venganza o humillación.

Observamos entonces, en el segundo caso, la criminalización del fenómeno de *revenge porn* o traducido como, pornografía de venganza, se caracteriza por una transgresión de la intimidad de la mujer mediante la exposición no autorizada de imágenes íntimas y que solía ser subsumido en el crimen de injuria previsto en el artículo 140 del Código Penal.

> Sin embargo, a partir de septiembre de 2018, con la inserción del artículo 218-C en el CP por la Ley 13.718/2018, el *revenge porn* pasó a ser previsto autónomamente, como respuesta al aumento del crimen de difusión o divulgación de escenas de violación o violación de vulnerables, escenas de sexo y/o pornografía.

Por último, en el segundo párrafo se prevé la exclusión de la ilegalidad al establecer que no existe delito cuando el agente practica la conducta descrita en una publicación periodística, científica, cultural o académica con la adopción de un recurso que hace imposible la identificación de la víctima, salvo con su autorización previa, si es mayor de 18 años.

Infiltración de agentes

En todo este contexto que estamos abordando, es importante señalar que la **Ley 13.441/2017**, que modificó el Estatuto de la Niñez y la Adolescencia (ECA), logró autorizar expresamente infiltración de agentes de policía en *internet*, con el objetivo de investigar delitos contra la dignidad sexual de niños, niñas y adolescentes.

Saber más

La Ley 13.441/2017 es la tercera disposición legislativa para la infiltración de agentes, que ya existía en el artículo 53 inciso I de la Ley 11.343/2006 (Ley de Drogas) y en el artículo 10 de la Ley de Delincuencia Organizada (Ley 12.850/2013).

Para acceder a ella en su totalidad, haz clic en el siguiente *link*: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm

En particular, la Ley 13.441/2017 introdujo la Sección V-A en el Capítulo II de la ECA. Pues bien, el artículo 190-A del ECA, introducido por la Ley 13.441/2017, establece que la infiltración de agentes de policía en *internet* puede producirse para investigar los siguientes delitos, que identificamos en la siguiente imagen:

> Producir, filmar, grabar una escena de sexo explícito o pornográfico que involucre a un niño, niña o adolescente (Art. 240 del ECA).

> Vender un video que contenga una escena sexual explícita o pornográfica que involucre a un niño o adolescente (Art. 241 ECA).

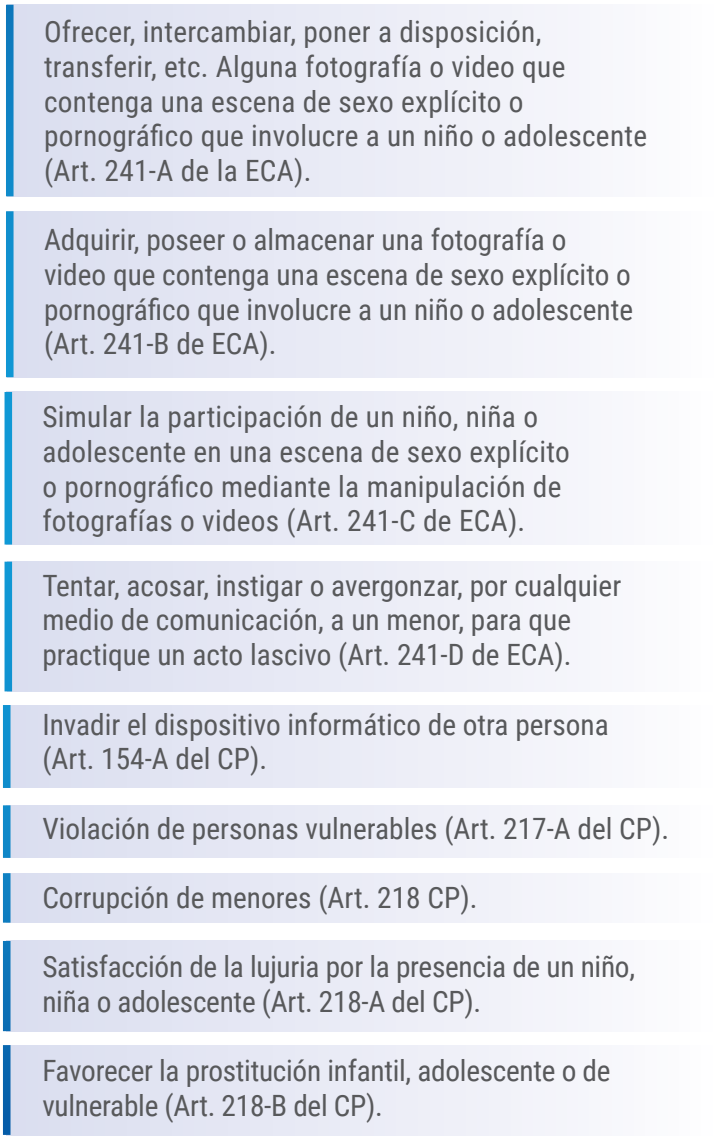


Figura 34: Delitos tipificados en el artículo 190-A del ECA. **Fuente:** labSEAD-UFSC (2020).

Esta infiltración sólo será lícita si está previamente autorizada por una decisión judicial debidamente detallada y motivada, que establecerá los límites de la infiltración para obtener pruebas. Sin embargo, la infiltración de agentes sólo será autorizada por el juez sobre una base subsidiaria. Es decir, no se permitirá la infiltración de agentes de policía en *internet* si se pueden obtener pruebas por otros medios (artículo 190-A, párrafo tercero del ECA).

Por lo tanto, la infiltración de la policía debe considerarse el *ultima ratio* (último ratio), es decir, es una prueba subsidiaria. La infiltración será evaluada por el juez, siempre que tenga origen en:

- Solicitudes del Ministerio Público.
- Representación del Jefe de Policía.

Veamos, en la siguiente imagen, qué se debe demostrar en la aplicación que solicita la infiltración.

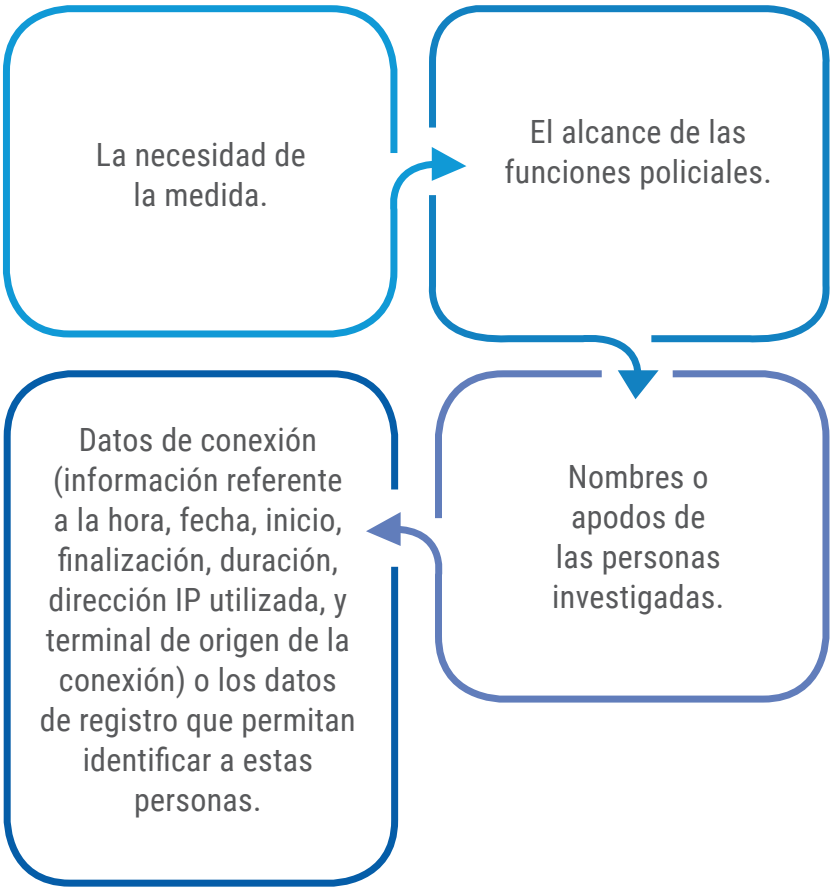


Figura 35: Información presente en la solicitud de infiltración. **Fuente:** labSEAD-UFSC (2020).

Otro detalle es que esta **infiltración tiene término**. La infiltración no puede exceder el período de noventa días, pudiendo renovarse sucesivamente si es necesario. Sin embargo, aunque se permiten renovaciones sucesivas, existe un límite: **el período total de infiltración no puede ser superior a setecientos veinte días**.

> El ECA también permite, en el artículo 190-D, la creación de una **"identidad ficticia"**, para que el agente infiltrado pueda utilizarla durante la infiltración, a través de la *internet*, con el fin de reunir pruebas sobre la autoría y veracidad de los crímenes investigados durante la infiltración.

El ECA también prevé que la identidad ficticia del policía infiltrado no configura un crimen. Sin embargo, si un policía encubierto, se extralimita en sus prácticas, deberá responder por los excesos cometidos.

> Una vez concluida la investigación, todos los actos electrónicos realizados durante la operación deben ser registrados, grabados, almacenados y remitidos por el jefe de la policía al juez, y al Ministerio Público, junto con un informe detallado.

Este informe final detallado no impide que la autoridad judicial y el fiscal soliciten informes parciales sobre la operación de infiltración antes de que expire el plazo de la medida. Por último, cabe señalar que el ECA establece que la infiltración es llevada a cabo por "agentes de la policía" (artículo 190A del ECA).

En este contexto, sólo la **Policía Federal y la Policía Civil** son los órganos que abarcan la función de policía investigadora, mientras que el resto de los órganos de seguridad pública, sólo ostentan la función de policía ostensible.

Así, sólo los agentes de la Policía Federal y de la Policía Civil pueden actuar como agentes encubiertos o infiltrados de acuerdo con el artículo 190-A del Estatuto de la Niñez y la Adolescencia (ECA, en portugués).

Finalmente, dado Por último, en vista de todo lo que hemos aprendido hasta ahora, podemos concluir que Brasil no tiene una legislación consolidada sobre *internet*,y mucho menos una legislación consolidada sobre crímenes digitales. Lo que tenemos son caracterizaciones de delitos cibernéticos propios extendidos por todo el Código Penal y otras leyes.

Las normas mencionadas son suficientes para proporcionar una base teórica y jurídica para hacer frente al fenómeno de

la delincuencia cibernética en la Seguridad Pública de Brasil. Adicionalmente, existen otras leyes en materia de *internet* y dispositivos informáticos, como la Ley General de Protección de Datos Personales, Ley 13.709, de 14 de agosto de 2018, que prevé el procesamiento de datos personales en el entorno virtual.

Saber más

Para obtener más información sobre la Ley 13.709/2018, haz clic en el siguiente *link*:

Ley General de Protección de Datos de Carácter Personal – http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art60

A fin de cuentas, toda la legislación relativa a la *internet* y los dispositivos informáticos repercute en la seguridad pública y no debe pasarse por alto. Así pues, la identificación de estos delitos existentes por la legislación del país nos ayudará a desarrollar una base que contribuya para los procesos de investigación relacionados con los delitos electrónicos.

Referencias

BARRETO, A. G.; BRASIL, B. S. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

BRASIL. [Constituição de 1988]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 15 jul. 2020.

BRASIL. **Decreto-Lei n.º 2.848, 7 de dezembro de 1940.** Código Penal. Brasília, DF: Presidência da República, [2019a]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 jul. 2020.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, DF: Presidência da República, [2019b]. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, Presidência da República, 2019c. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 10.446, de 8 de maio de 2002**. Dispõe sobre infrações penais de repercussão interestadual ou internacional. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10446.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.830, de 20 de julho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.737, 30 de novembro de 2012**. [Lei Carolina Dieckmann]. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. [Marco Civil da Internet]. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 13.260, de 16 de março de 2016.** [Lei Antiterrorismo]. Brasília, DF, Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em 15 jul. 2020.

BRASIL. **Lei n.º 13.441, de 8 de maio de 2017.** Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na *internet* com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Brasília, DF, Presidência da República, 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Acesso em: 15 jul. 2020.

BRASIL. Superior Tribunal de Justiça. **REsp 1193196 MG 2010/0084049-5.** Relator: Ministra Maria Tereza de Assis Moura. Recorrente: Ministério Público do Estado de Minas Gerais. Recorrido: Emília Aparecida Borges. 26 set. 2012. Brasília, DF, 2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/22896028/recurso-especial-resp-1193196-mg-2010-0084049-5-stj/inteiro-teor-22896029. Acesso em: 15 jul. 2020.

FLATICON. [*S.l.*], 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 16 jul. 2020.

PIXABAY. [*S.l.*], 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 16 jul. 2020.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 14 jul. 2020.

WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. **G1**, São Paulo. 19 jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 15 jul. 2020.

MÓDULO 5

INVESTIGACIÓN DE CRÍMENES ELECTRÓNICOS EN BRASIL

Presentación

La investigación de los delitos cibernéticos es, ante todo, la investigación de un delito y, aunque tiene características específicas, debe llevarse a cabo siguiendo los protocolos, normas y procedimientos de una investigación penal común.

En este módulo, aprenderemos primero los aspectos generales de la investigación policial y, más adelante, los aspectos específicos de la investigación de los delitos cibernéticos en Brasil.

OBJETIVOS DEL MÓDULO

Conocer las bases teóricas y jurídicas que integran los aspectos generales de la investigación policial y los aspectos específicos de la investigación de los delitos cibernéticos.

ESTRUCTURA DEL MÓDULO

- **Clase 1 –** Investigación Policial.
- **Clase 2 –** Investigación de Delitos Cibernéticos.

Clase 1 – Investigación Policial

CONTEXTUALIZANDO...

Todavía en el contexto de la legislación brasileña relativa a los delitos digitales, conoceremos ahora los aspectos generales de una investigación policial que, por regla general, corresponde a la policía judicial.

¿Sabes lo que define a una policía judicial en Brasil?

Es por este tema que daremos inicio a la clase de investigación policial.

¡Vamos!

ATRIBUCIÓN LEGAL PARA INVESTIGAR

La policía, en una perspectiva amplia, es el órgano a través del cual el Estado promueve la seguridad pública. Y, por regla general, en Brasil, la investigación criminal es responsabilidad de la policía judicial.

En este sentido, destacamos los aspectos generales de la investigación policial, es decir, los objetos considerados para caracterizar a la policía en Brasil según la legislación.

Figura 1: Caracterización de la seguridad pública en Brasil. **Fuente:** labSEAD-UFSC (2020).

Podemos ver que la investigación criminal es responsabilidad de la Policía Civil y de la Policía Federal y así lo establece el artículo 4 del Código Procesal Penal (CPP).

Veamos qué dice el artículo:

> *Artículo 4º - La policía judicial será ejercida por las autoridades policiales en el territorio de sus respectivas circunscripciones y tendrá por objeto establecer los delitos y su autoría. (BRASIL, 2019, traducción nuestra).*

De manera excepcional y puntual, otras fuerzas policiales también pueden investigar, como sucede con la Policía Legislativa (en el caso de delitos cometidos en el parlamento) y la Policía Militar (en el caso de delitos militares cometidos por sus miembros). Por lo tanto, como norma, según lo dispuesto en la Constitución Federal (CF) y la Ley 12.830/2013, **la actividad de la policía judicial es exclusiva de la Policía Federal y de la Policía Civil, y es esencial y exclusiva del Estado.**

Veamos, respectivamente, las disposiciones de la Constitución Federal y de la Ley 12.830/2013 que tratan del tema.

> *Art. 144 - IV - Ejercer, con carácter exclusivo, las funciones de la policía judicial de la Unión. (BRASIL, 2020, traducción nuestra).*

> *Artículo 2º - Las funciones de la policía judicial y la investigación de los delitos penales que lleva a cabo el agente de policía son de naturaleza jurídica, esenciales y exclusivas del Estado. (BRASIL, 2013 traducción nuestra).*

Ante esto, a continuación, conoceremos cómo la Policía Civil y la Policía Federal comparten esta tarea de investigar delitos.

Atribuciones de investigación de la Policía Civil y de la Policía Federal

Como vimos anteriormente, aunque de manera excepcional y puntual, otras fuerzas de policía también pueden investigar. La Constitución Federal, el Código Procesal Penal y la Ley 12.830/2013 atribuyen la actividad de policía judicial, es decir, la actividad de investigación, con exclusividad a la Policía Federal y a la Policía Civil.

Así pues, veremos ahora cómo la Policía Federal y la Policía Civil comparten esta atribución de investigar, especialmente en lo que respecta a los delitos cibernéticos.

Policía Federal

De conformidad con la Constitución Federal y la Ley 13.260/2016, la Policía Federal está destinada a algunas actividades específicas.

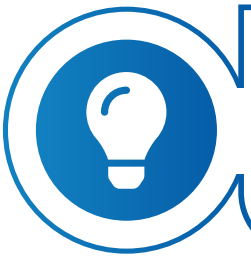
Conozcámoslos en la siguiente imagen:

Figura 2: Atribuciones de la Policía Federal. **Fuente:** labSEAD-UFSC (2020).

En lo que respecta a esta lista de funciones, además de las funciones de la policía marítima, aeroportuaria y fronteriza (que es una función administrativa), las demás consisten

en las **atribuciones de investigación** de la Policía Federal. Todavía en relación con estas actividades, un punto que merece destacarse es la **atribución de la Policía Federal de "investigar otras infracciones cuya práctica tenga repercusiones interestatales o internacionales y requiera una represión uniforme, de acuerdo con la ley".**

A este respecto, es importante saber que la Constitución Federal no aclara cuáles son los delitos penales con repercusiones interestatales o internacionales que requieren una represión uniforme. Esto se hace por la **Ley 10.446/2002**. Esta ley establece que la Policía Federal se encarga de investigar los siguientes delitos porque son delitos penales con repercusiones interestatales o internacionales que requieren una represión uniforme.



Saber más

Puedes mejorar tus conocimientos accediendo a la Ley 10.446/2002 completa, disponible en el *link*: http://www.planalto.gov.br/ccivil_03/leis/2002/l10446.htm

Ahora, conoceremos los delitos investigados por la Policía Federal, según la Ley 10.446/2002. Observa la imagen a continuación:

Secuestro, prisión privada y extorsión por secuestro (artículos 148 y 159 del Código Penal), si el autor fue impulsado por razones políticas o cuando se realiza como resultado del servicio civil ejercido por la víctima.

Formación de un cártel (artículos I, a, II, III y VII del art. 4 de la Ley 8.137, de 27 de diciembre de 1990).

Acciones relacionadas con violaciones de los derechos humanos, que la República Federativa del Brasil se ha comprometido a reprimir como resultado de los tratados internacionales en los que es parte.

Robo, hurto o recepción de carga, incluidos bienes y objetos de valor, transportados en operaciones interestatales o internacionales, cuando haya pruebas de la acción de una banda o de un grupo en más de un estado de la Federación.

Falsificación, corrupción, adulteración o alteración de un producto destinado a fines terapéuticos o medicinales y venta, incluso a través de internet, depósito o distribución del producto falsificado, corrompido, adulterado o alterado (Artículo 273 del Decreto-Ley 2.848 del 7 de diciembre de 1940 - Código Penal).

Robo, hurto o daños contra instituciones financieras, incluidas las sucursales bancarias o los cajeros automáticos, cuando haya pruebas de asociación delictiva en más de un estado de la Federación.

Cualquier delito cometido a través de la World Wide Web que difunda contenido misógino, definido como aquellos que propagan el odio o la aversión a las mujeres.

Figura 3: Delitos investigados por la Policía Federal, según la Ley 10.446/2002.
Fuente: labSEAD-UFSC (2020).

Además, cuando haya repercusiones interestatales o internacionales que requieran una represión uniforme, el Departamento de Policía Federal del Ministerio de Justicia podrá, sin perjuicio de la responsabilidad de otros organismos

de seguridad pública, proceder a investigar otros casos, siempre que tal acción sea autorizada o determinada por el Ministro de Estado de Justicia y Seguridad Pública.

Así pues, la Policía Federal puede investigar otras infracciones penales que no figuran en esta lista, siempre que:

- Dicha medida sea autorizada o determinada por el Ministro de Estado de Justicia y Seguridad Pública.
- La infracción tenga repercusiones interestatales o internacionales y requiera una represión uniforme.

De todas estas atribuciones de investigación de la Policía Federal se desprende que el legislador se ha ocupado expresamente de los delitos electrónicos al ordenar a la Policía Federal que investigue todos los delitos cometidos a través de la World Wide Web que difundan contenidos misóginos, definidos como los que **propagan el odio o la aversión a la mujer.**

La Policía Federal tiene muchas atribuciones, pero cuando se trata de delitos cibernéticos (los que se cometen exclusivamente en un entorno virtual), estas atribuciones pueden enumerarse de acuerdo con lo que vemos en la imagen siguiente.

Figura 4: Delitos cibernéticos investigados por la Policía Federal.
Fuente: labSEAD-UFSC (2020).

Con respecto a los delitos cibernéticos que se consideran delitos federales, la Constitución Federal, en su artículo 109, expone una larga lista de situaciones que caen dentro de la jurisdicción federal. De esta larga lista, es de interés el inciso V del mismo artículo, que establece que los delitos previstos en un tratado o convención internacional son de la competencia de la Justicia Federal, cuando, al iniciarse la ejecución en el país, el resultado se ha producido o debió producirse en el extranjero, o en forma recíproca.

Se trata de una disposición estrechamente relacionada con los delitos digitales, ya que es relativamente común que personas de otros países, a través de *internet*, cometan delitos en Brasil y viceversa.

Saber más

Con el fin de establecer el Estado democrático y garantizar el ejercicio de los derechos del pueblo brasileño, se dio la Constitución de la República Federativa del Brasil de 1988. Ya que estamos destacando su importancia en el contexto de las atribuciones de la Policía Federal, haz clic en el siguiente *link* y conócela mejor.

Constituição da República Federativa do Brasil - http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

En resumen, para que el delito cometido a través de *internet* sea juzgado por el Tribunal Federal (e investigado por la Policía Federal), debe encajar en una de las hipótesis enumeradas en el artículo 109, cláusulas IV y V de la Constitución Federal.

En la figura a continuación se enumeran las hipótesis enumeradas en el artículo 109/CF, puntos IV y V, en forma resumida.

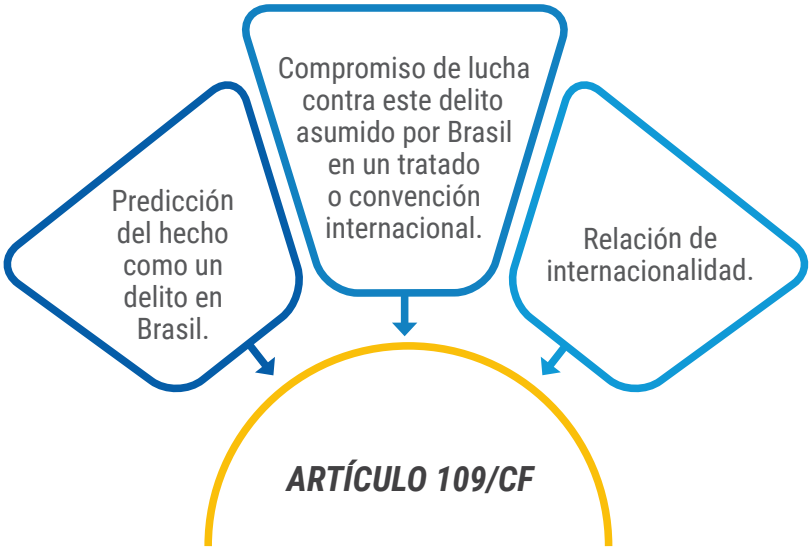


Figura 5: Hipótesis enumeradas en el artículo 109 de la Constitución Federal. **Fuente:** labSEAD-UFSC (2020).

Cuando se dan estas hipótesis, la Policía Federal se encarga de investigar estos delitos. Así, por ejemplo, en el caso de un delito de **racismo practicado por *internet*, la investigación será de la Policía Federal**, porque el racismo está previsto como delito en Brasil y es un delito que Brasil se comprometió a **reprimir sobre la base de los tratados internacionales.** Además, la difusión de mensajes racistas en *internet* puede ser vista por cualquier persona en el mundo. Así pues, se cumplen los tres requisitos mencionados y la competencia recae en la Justicia Federal. Otros ejemplos de delitos que Brasil se comprometió a combatir son: la xenofobia, la publicación de pornografía infantil, entre otros.

Saber más

En este contexto, para acceder al artículo 109 de la Constitución Federal en su totalidad, haz clic en el *link*: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

En el caso de los **delitos de injuria** cometidos a través de la World Wide Web, **no hay delitos de la competencia de la Policía Federal**, ya que el delito de injuria **no está previsto en un tratado o convención internacional. Por lo tanto, el delito de injuria no entra en el punto V del artículo 109.**

Figura 6: Delitos de injuria a través de la World Wide Web. **Fuente:** Pixabay (2020).

Para reflexionar sobre los delitos de injuria cometidos a través de la World Wide Web, observemos el análisis propuesto en la siguiente secuencia.

En la Práctica

Así, por ejemplo, en el Conflicto de Jurisdicción 111.338/TO, hubo difusión de imágenes pornográficas, involucrando niños y adolescentes a través de la red social Orkut, probablemente no restringida a una comunicación electrónica entre personas residentes en Brasil y es un delito previsto en un tratado o convención internacional (Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas, aprobada por el Decreto Legislativo 28/1990 y el Decreto 99.710/1990), por lo que el Supremo Tribunal de Justicia (STJ) consideró que era un delito de la competencia de la Justicia Federal.

Sin embargo, en otro Conflicto de Jurisdicción (CC 99.133/SP) juzgado por el STJ, el Tribunal evaluó un caso de intercambio, por *e-mail*, de imágenes pornográficas de niños entre dos personas que vivían en Brasil, ya que en este caso se demostró que el delito de divulgación de escenas pornográficas que involucraban a niños no traspasaba las fronteras del Brasil y quedaba restringido a los

intercambios de *e-mail* entre las dos personas investigadas que vivían en Brasil. Así, el STJ consideró que no se cumplía el requisito de una relación internacional y consideró que la jurisdicción para juzgar el caso era el Tribunal del Estado.

Dadas las facultades de investigación de la Policía Federal, especialmente en relación con los delitos cibernéticos, veremos ahora cuáles son las facultades de investigación de la Policía Civil en Brasil.

Policía Civil

En cuanto a la Policía Civil, la Constitución Federal establece que, salvo la competencia de la Unión, las funciones de la policía judicial y la investigación de las infracciones penales, excepto las militares, deben ser cumplidas por ella.

> Esto significa que la Policía Civil tiene atribuciones subsidiarias en relación con la Policía Federal. Por lo tanto, corresponde a la Policía Civil investigar todo lo que no figure como atribución de la Policía Federal, es decir, corresponde a la Policía Civil investigar la mayoría de los delitos tipificados por la legislación brasileña.

En lo que respecta a los delitos cibernéticos, en general, dado el carácter subsidiario de las funciones de la Policía Civil, les corresponde investigar la mayoría de los delitos cometidos en un entorno virtual o a través de él.

Así, podemos conocer las atribuciones de la Policía Federal y Civil en Brasil, principalmente en el cumplimiento relacionado con los delitos electrónicos.

Ahora, siguiendo nuestros estudios, detallaremos el proceso de investigación de estos delitos en la siguiente clase.

Clase 2 – Investigación de Delitos Cibernéticos

CONTEXTUALIZANDO...

Aunque la investigación de los delitos digitales tenga sus matices y especificidades, se trata de una investigación penal y, por lo tanto, sigue los protocolos, normas y procedimientos de una investigación penal común.

Ya conocemos las atribuciones de investigación de la Policía Civil y Federal relacionadas con los delitos cibernéticos, ahora conoceremos el flujo de procesos de investigación de la tipología de este delito en Brasil.

EL PROCESO DE INVESTIGACIÓN

Como en la investigación de cualquier delito, la investigación de delitos cibernéticos pasa por las dos etapas típicas de la investigación penal: la **investigación preliminar** y la **investigación de seguimiento.**

Las identificamos en la siguiente imagen.

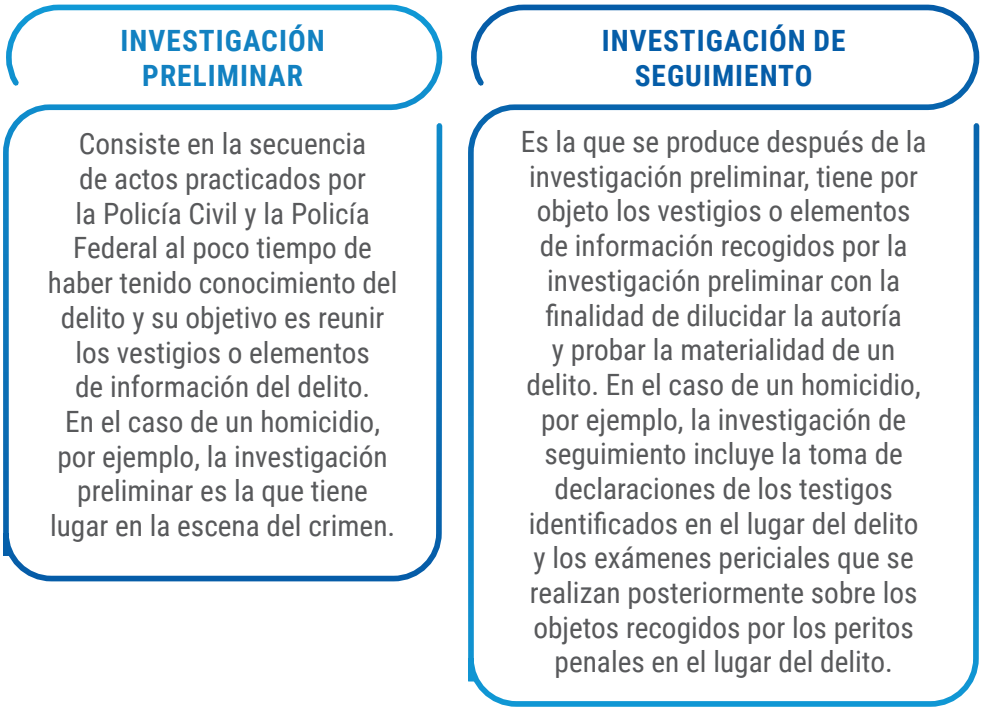


Figura 7: Investigación preliminar y de seguimiento. **Fuente:** labSEAD-UFSC (2020).

A pesar de esta conceptualización, no hay una delimitación clara en la doctrina de la investigación en cuanto a cuándo se completa la investigación preliminar y cuándo comienza la investigación de seguimiento. Así que, conozcamos en detalle la investigación preliminar de los delitos cibernéticos.

Investigación preliminar de delitos cibernéticos

Como vimos, la investigación preliminar consiste en actos practicados por la Policía Civil y por la Policía Federal poco después de haber tenido conocimiento del delito, cuya finalidad es reunir los vestigios o elementos de información originados por el delito. En este sentido, hay una serie de actos que debe practicar el oficial de policía tan pronto como tenga conocimiento del delito.

Veamos lo que dice el artículo sexto del Código Procesal Penal (CPP):

> *Art. 6º - establece una verdadera hoja de ruta de los actos que deben preceder al establecimiento de la investigación policial. (BRASIL, 2019, traducción nuestra).*

Por lo tanto, **tan pronto como la autoridad policial esté al tanto de la práctica del delito**, debe promover algunas acciones, que podemos ver en la siguiente imagen.

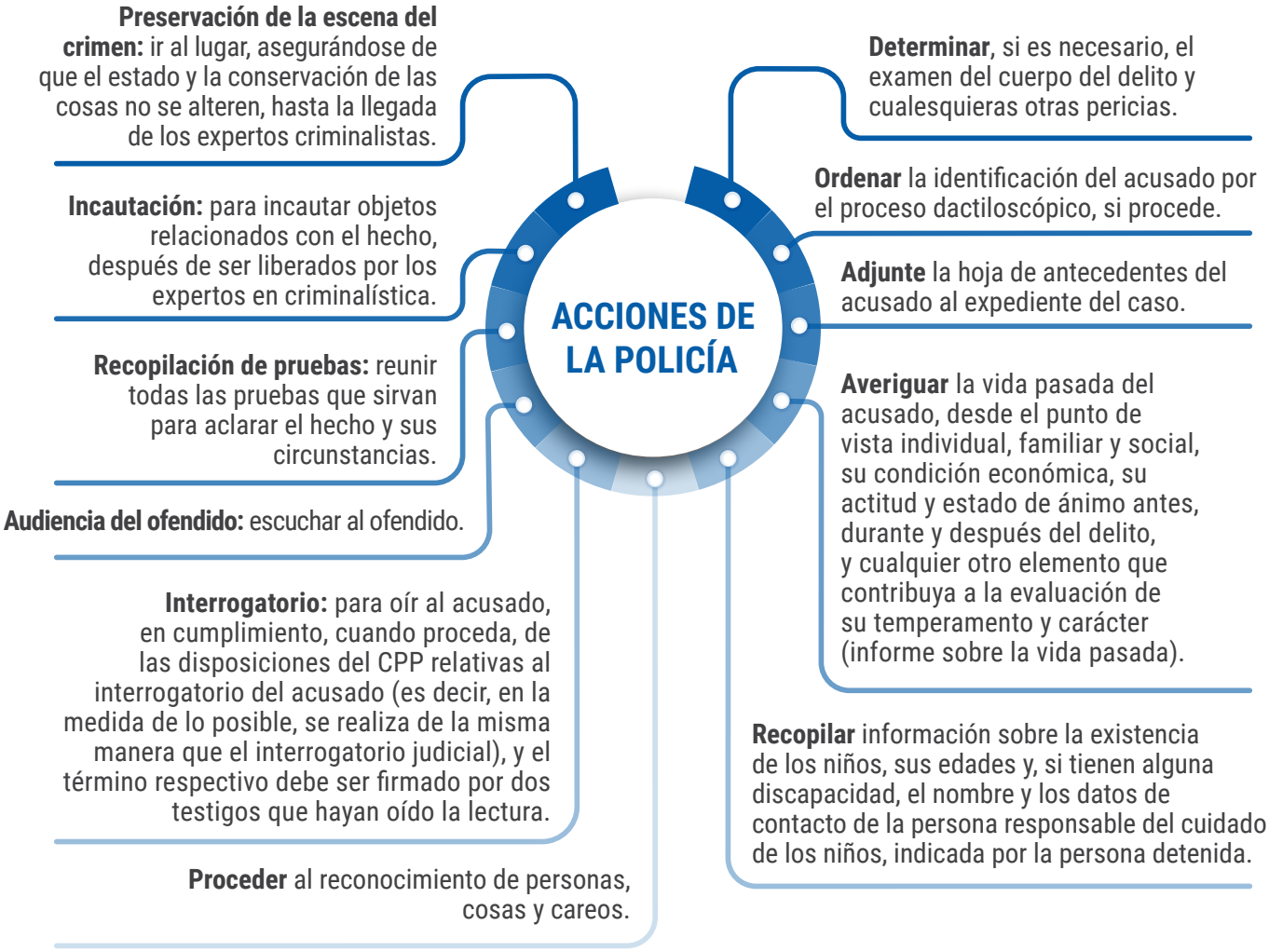


Figura 8: Acciones policiales tras el conocimiento de la práctica del delito. **Fuente:** labSEAD-UFSC (2020).

Cabe señalar que estas acciones que acabamos de ver no son exhaustivas y que no es necesario que todas ellas se realicen o se lleven a cabo en este orden. Así, al trasladar estas directrices a la investigación preliminar de los delitos digitales, se verifican algunos problemas.

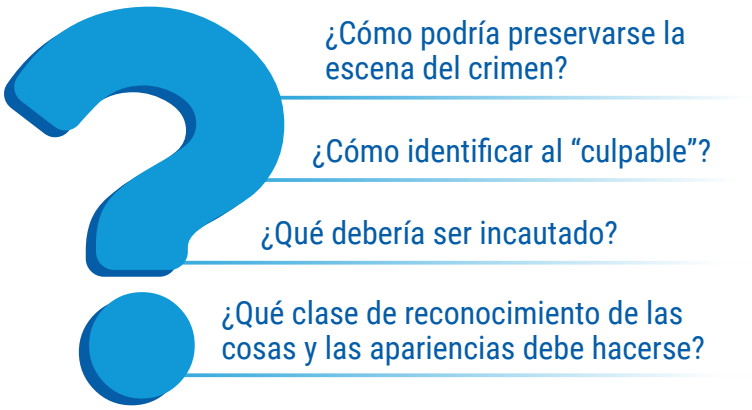


Figura 9: Preguntas relacionadas con la investigación de los delitos cibernéticos. **Fuente:** labSEAD-UFSC (2020).

El intento de responder a estas preguntas lleva a la conclusión de que la hoja de ruta de los actos que deben preceder a la iniciación de una investigación policial, establecida en el artículo 6 del Código Procesal Penal (CPP), no parece encajar bien con la investigación preliminar del delito electrónico. De hecho, esto es lo que sucede, entre otras cosas porque el CPP es un documento normativo que se remonta a 1941.

Por lo tanto, las directrices del artículo 6 del CPP deben transponerse y adaptarse a la realidad de los delitos cibernéticos, adaptándose a las características y peculiaridades de este tipo de delitos.

> A modo de ejemplo, un detalle que se puede observar es que, la mayoría de las veces, ni siquiera se tiene un sospechoso, ya que la principal característica de *internet*, cuando se trata de cometer delitos, es la posibilidad del anonimato.

Por lo tanto, en la mayoría de los casos de delitos cibernéticos, no hay ningún elemento que permita calificar e identificar inmediatamente al autor del delito. Es decir, los medios enumerados en el artículo 6º del CPP: reconocimiento de personas y cosas, interrogatorio del sospechoso.

Pero entonces, ¿cómo emprender la investigación preliminar de los delitos cibernéticos ante las peculiaridades de este tipo de delitos?

En el caso de los delitos digitales, la investigación preliminar trata de lograr algunos propósitos. Vamos a conocerlos en la siguiente imagen.

Figura 10: Propósitos de la investigación preliminar. **Fuente:** labSEAD-UFSC (2020).

Ahora que conocemos estos propósitos, comprenderemos más sobre sus especificidades.

Identificación del medio o servicio de *internet* empleado

La primera preocupación de los agentes de la Policía Civil o de la Policía Federal en la investigación preliminar, cuando se enfrentan a un delito digital, es identificar el medio o servicio de *internet* empleado. **Toda la planificación de una investigación de un delito cibernético depende en gran medida de la identificación del medio o servicio de *internet* empleado.**

> Identificar el medio o servicio de *internet* empleado es identificar el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet* cuyos servicios sirvieron de instrumento para cometer el delito.

Como ya vimos, se enumeraron las atribuciones de investigación de la Policía Federal y se dieron dos ejemplos en relación con los conflictos de competencia 111.338/TO y 99.133/SP. Recordando: el CC 111.338/TO se refería a la publicación de fotografías con contenido pornográfico infantil en noviembre de 2008 a través de una página de la red social Orkut (hoy desactivada). Es decir, se trataba del delito del artículo 241-A del Estatuto del Niño y del Adolescente (ECA). **En la investigación preliminar de esos delitos, uno de los primeros pasos es identificar el proveedor de aplicaciones de *internet* que contribuyó a la comisión de los delitos. En el caso, la red social Orkut.**

El CC 99.133/SP implicaba a un investigado que habría practicado varios actos libidinosos de la conjunción carnal con su hija y publicado las escenas pornográficas en *internet* mediante el uso de *webcam* y mensajes. A continuación, se investigó la práctica de los delitos previstos en los artículos 214, 224 y 226, apartado II, todo el Código Penal Brasileño (agresión violenta a las buenas costumbres con presunta violencia cometida por ascendiente) y el artículo 241, caput de la Ley 8069/1990 (divulgación de material pornográfico en el que participen niños o adolescentes), en un concurso de materiales (artículo 69 del CPB). **Pues bien, en la investigación preliminar de esos delitos, uno de los primeros pasos es identificar al proveedor de aplicaciones de *internet* que fue decisivo en la práctica de los delitos y que se utilizó para transmitir los mensajes e imágenes de la *webcam*.**

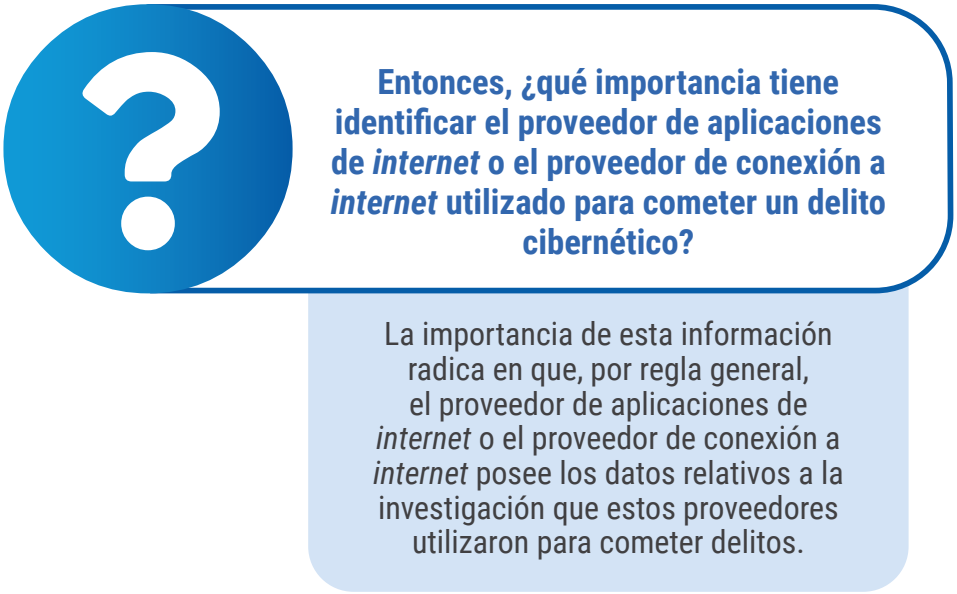


Figura 11: La importancia de identificar al proveedor de aplicaciones de *internet*. **Fuente:** labSEAD-UFSC (2020).

Por consiguiente, al identificar al proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet*, se pueden solicitar datos a estos proveedores en la fase de investigación de seguimiento. Estos datos culminarán entonces en la identificación de los autores de los delitos electrónicos investigados.

> En resumen, la identificación de los responsables del servicio de *internet* implicados es fundamental en la investigación preliminar, de modo que en la fase de investigación de seguimiento se puedan solicitar datos a estos proveedores de servicios.

Por lo tanto, en la investigación preliminar de un delito contra el honor cometido a través de una red social, se debe:

Paso 1 – Identificar qué red social está involucrada. Es decir, deberías comprobar si es Facebook, Instagram, LinkedIn, Snapchat, WeChat, TikTok o muchos otros. También, en la hipótesis de los delitos cibernéticos practicados en los chats, donde hay que verificar cuál es el proveedor de este servicio (UOL, Terra etc.).

Paso 2 – En el caso de las aplicaciones de mensajería que han sido utilizadas como herramienta para estos delitos, se debe investigar qué compañía está involucrada (WhatsApp, Telegram, Signal, Skype, Hangout etc.). Si el delito cibernético se cometió por *e-mail*, hay que observar qué proveedor de servicios de *e-mail* está involucrado. Entre ellos, podemos ejemplificar con Gmail, Yahoo, ProtonMail, Hotmail y otros. De la misma manera, si el delito involucra un *website*, se debe identificar cuál es la compañía de *internet* que lo aloja (GoDaddy, Locaweb, HostGator etc.).

En algunos casos, es obvio identificar el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet* cuyos servicios sirvieron de instrumento para cometer el delito cibernético. Este es el caso, por ejemplo, de las redes sociales y las aplicaciones de mensajería.

Figura 12: Redes sociales y páginas donde se cometen delitos cibernéticos.
Fuente: Pixabay (2020).

En otros casos, esta identificación depende de la realización de algunos procedimientos, como es común en la identificación de empresas de *internet* que albergan sitios *web* o en el intento de identificar algunos proveedores de servicios de *e-mail* (especialmente en el caso de ***spoofing***).

Casos de encubrimiento de remitentes de e-mail.

Los procedimientos que se adopten en esos casos dependen de un curso práctico de investigación de delitos electrónicos y quedan fuera del alcance de este curso teórico.

Procedamos entonces a conocer cómo se preservan los vestigios del delito.

Preservación de los vestigios del delito

Una vez identificado el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet*, cuyos servicios sirvieron de instrumento para cometer el delito, el siguiente paso es preservar los vestigios del delito.

En el caso de los delitos comunes, la conservación de los vestigios consiste esencialmente en la preservación del lugar del delito y la incautación de los instrumentos o productos

del delito. Así, por ejemplo, en el caso de un homicidio, la preservación de los vestigios se produce de cierta manera. Vamos a identificarlo en la siguiente imagen.

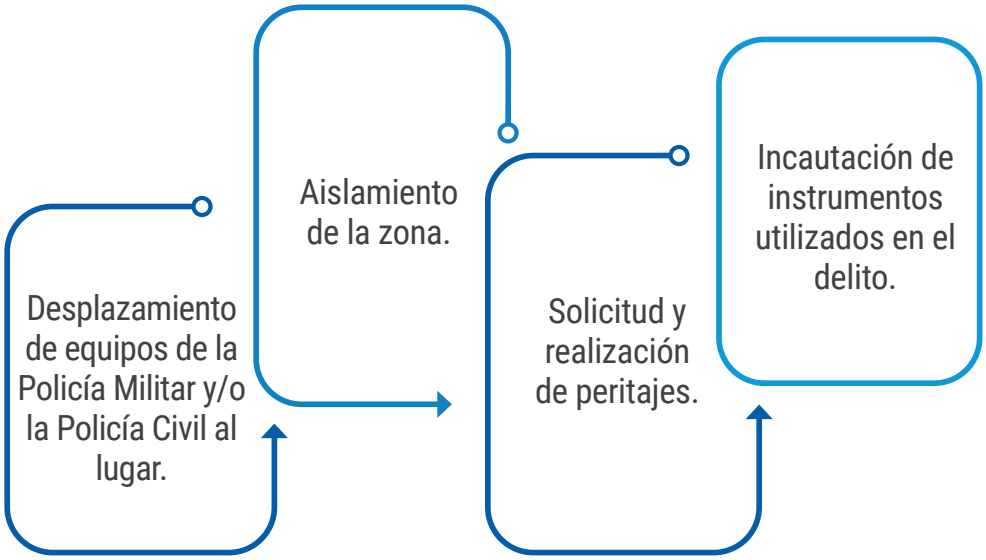


Figura 13: Preservar los vestigios de la escena de un delito de homicidio. **Fuente:** labSEAD-UFSC (2020).

En la investigación preliminar de los delitos cibernéticos deben aplicarse procedimientos similares a los que vimos en la figura anterior. Sin embargo, salvo en casos concretos, los vestigios dejados por la delincuencia digital se localizan en un **entorno virtual,** no en el mundo físico.

¿Cómo, entonces, debes operar el aislamiento y la preservación de los vestigios localizados en un entorno virtual y relacionados con estos delitos?

La preservación de los vestigios digitales de los delitos electrónicos tiene dos etapas. Conócelas en la imagen de abajo.

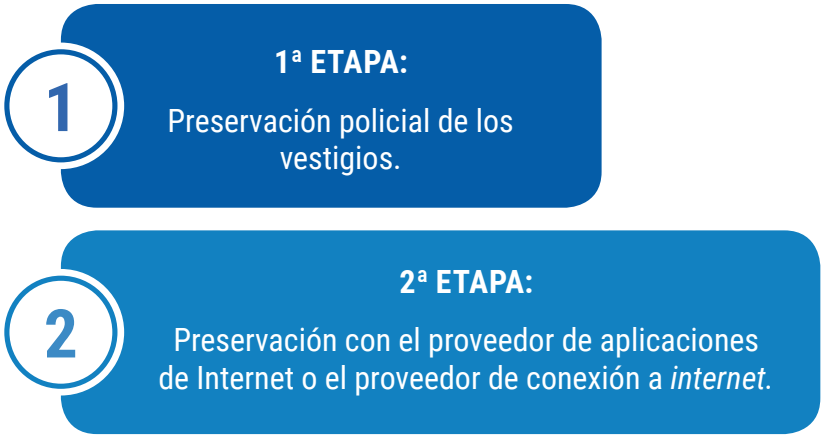


Figura 14: Etapas de la preservación de vestigios en la investigación de delitos digitales. **Fuente:** labSEAD-UFSC (2020).

En lo que respecta a la primera etapa de la preservación de vestigios en la investigación de los delitos cibernéticos, **la preservación policial de los vestigios**, podemos considerar algunas opciones dependiendo del caso concreto que se investigue. La conservación policial de los vestigios **puede hacerse mediante un certificado policial, un notario público, la adquisición forense de vestigios y un examen pericial.**

En cuanto a la segunda etapa de la **preservación, que es la preservación con el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet*, no siempre será posible** porque, como vimos anteriormente, la manera de promover eficazmente la preservación con el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet* varía de una empresa a otra. Por ejemplo, WhatsApp, Facebook e Instagram tienen una plataforma para solicitar la conservación. Por otra parte, la empresa Tinder no dispone de una plataforma específica para ello, por lo que se debe enviar un *e-mail* a la empresa solicitando la conservación de los datos de interés para la investigación.

Si bien la conservación policial de los vestigios materializa y preserva aspectos como textos, imágenes y vídeos a través de los cuales se propagan los delitos cibernéticos, no pueden preservar los datos de los delincuentes para acceder a las aplicaciones de *internet* o a los proveedores de conexión.

Imagina, por ejemplo, el caso de una injuria en un perfil de Facebook. En la conservación policial de los vestigios (1ª etapa), se hace una *printscreen* del mensaje injurioso seguida de un certificado policial. Este procedimiento preserva y materializa el delito, y también preserva la identificación del perfil del delincuente. Sin embargo, hay dos problemas que identificamos, analízalos en la imagen de abajo:

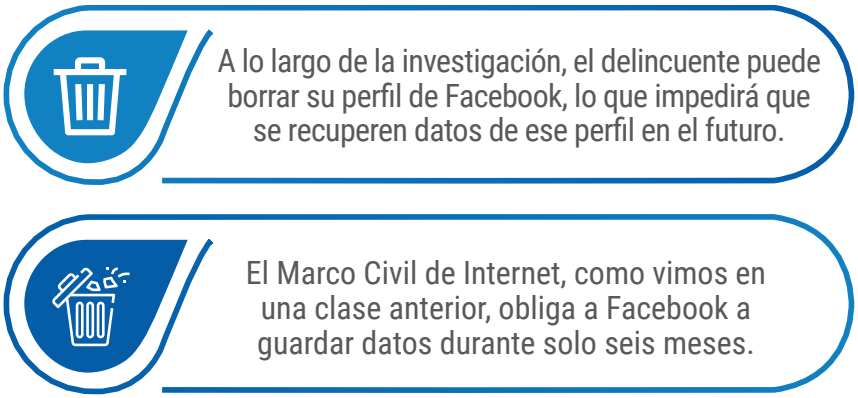


Figura 15: Situaciones encontradas en el caso de una injuria por un perfil de Facebook. **Fuente:** labSEAD-UFSC (2020).

Obsérvese que la preservación policial de los vestigios no puede proteger los datos del perfil del delincuente en este caso, que pueden ser eliminados por el propio delincuente o dejar de ser guardados por Facebook después de seis meses.

La salida para la conservación de estos datos es precisamente la segunda etapa del proceso de conservación con el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet* de los datos relacionados con el delito cibernético investigado.

Por lo tanto, seguimos nuestros estudios de la segunda etapa típica de la investigación del delito cibernético, la etapa de investigación de seguimiento.

Investigación de seguimiento

Una vez que se han identificado los medios o servicios de *internet* empleados en el delito cibernético y la conservación de los vestigios (mediante la conservación y preservación policial con el proveedor de aplicaciones de *internet* o el proveedor de conexión a *internet*), se pasa a la etapa de investigación de seguimiento.

> La investigación de seguimiento parte de todo lo planteado en la investigación preliminar y comienza a actuar con el propósito de reunir información que proporcione la materialidad de los delitos cometidos y permita llegar a la autoría de los mismos.

Cada investigación de un delito electrónico tiene sus peculiaridades e individualidades, pero se pueden esbozar algunas iniciativas que serán comunes en las investigaciones de delitos cibernéticos. En vista de ello, es común que todos los delitos digitales se cometan a través de un proveedor de aplicaciones de *internet* o de un proveedor de conexión a *internet*, por lo que es común hacer **solicitudes de datos** a estas empresas.

Por consiguiente, es necesario que en la investigación preliminar se identifique debidamente a esos proveedores y que se solicite la conservación de los datos de interés para la investigación.

Pero, después de todo, ¿cómo se lleva a cabo esta petición de solicitud?

En este punto, es necesario recordar que algunos detalles se cortan y no se tratan por separado. Vamos a conocerlos en la imagen siguiente.

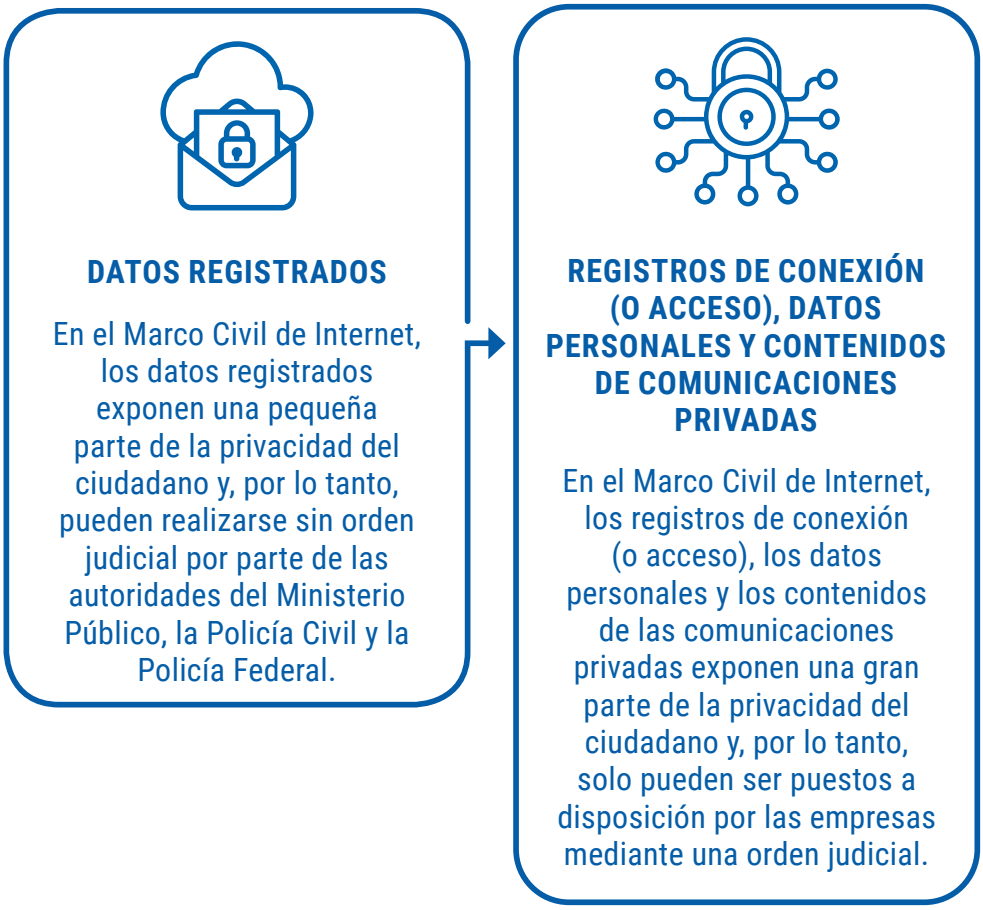


Figura 16: Tratamiento por separado de la solicitud de datos de interés para la investigación. **Fuente:** labSEAD-UFSC (2020).

Por lo tanto, las necesidades de datos registrados en la investigación de seguimiento se resuelven fácilmente, ya que esos datos pueden obtenerse de las empresas mediante una carta enviada por las autoridades del Ministerio Público, la Policía Civil y la Policía Federal.

> Así, por ejemplo, en el caso de un delito de difusión de material pornográfico infantil practicado por un perfil de Facebook, si interesa a la investigación de seguimiento obtener datos de registro de ese perfil, basta con una carta de las autoridades del Ministerio Público, la Policía Civil y la Policía Federal. En respuesta, Facebook puede poner a disposición, por ejemplo, el nombre introducido por el usuario, la fecha y la hora en que se creó el perfil, el *e-mail*, el número de teléfono y la dirección del protocolo de *internet* (IP- protocolo de *internet*) para crear la cuenta.

En ese contexto, comprenderemos más sobre las medidas de precaución en un entorno virtual.

Medidas de precaución en el entorno cibernético

Si es de interés para la investigación de seguimiento obtener el **historial de las direcciones IP** utilizadas por el autor para acceder a su perfil de Facebook, se requerirá una orden judicial que obligue a Facebook a enviar estos datos porque, como vimos anteriormente, en el caso de los registros de conexión (o de acceso), los datos personales y el contenido de las comunicaciones privadas, el Marco Civil de Internet establece que solo pueden ser puestos a disposición por las empresas **mediante una orden judicial.** Así que tenemos la figura de las **medidas de precaución en el entorno cibernético.**

Figura 17: Acceso a los datos del perfil del delito virtual en Facebook a través de una orden judicial. **Fuente:** Pixabay (2020).

El artículo 155 del Código Procesal Penal (CPP) exige que el juez formule su condena mediante la libre evaluación de las pruebas presentadas en un tribunal y no puede basar su decisión exclusivamente en la información reunida en la investigación. No obstante, el mismo artículo permite, excepcionalmente, que se utilicen pruebas extrajudiciales como elemento principal de la condena del juez. En otras palabras, se trata de una prueba de precaución, no sujeta a repetición y producida de antemano.

Las pruebas cautelares se guían por la necesidad y la urgencia, como en el caso de la interceptación telefónica, en la que se aplaza la contradicción. Pues bien, en la investigación de los delitos cibernéticos existen pruebas caracterizadas por la necesidad y la urgencia (pruebas de precaución) que son, precisamente, los registros de conexión (o acceso), los datos personales y el contenido de las comunicaciones privadas.

> La necesidad se caracteriza por el hecho de que sin esta información no es posible lograr la autoría de los delitos cibernéticos. Por otra parte, la urgencia se caracteriza por el hecho de que el Marco Civil de Internet estipula plazos estrictos para el almacenamiento de esta información por los proveedores de aplicaciones de *internet* y los proveedores de conexión.

Así pues, la representación ante el poder judicial para eliminar el secreto telemático de los objetivos de la investigación es parte integrante de la investigación del seguimiento de los delitos cibernéticos. A partir de ese momento, tenemos la representación ante el Poder judicial para la búsqueda y aprehensión en domicilio.

Estas representaciones para la eliminación del secreto y la confidencialidad de las comunicaciones telemáticas de los objetivos de la investigación se dirigen a los proveedores de aplicaciones de *internet* o a los proveedores de conexión a *internet*. Por lo tanto, conozcamos cómo se aplican estas medidas de precaución en un entorno virtual.

Cumplimiento de las medidas de precaución en el entorno cibernético

Los proveedores de aplicaciones de *internet* o el proveedor de la conexión a *internet*, al recibir la orden judicial, informan al organismo solicitante (Ministerio Público, Policía Civil y Policía

Federal) los registros de conexión (o de acceso), los datos personales y el contenido de las comunicaciones privadas.

Saber más

Los datos que serán comunicados por estos proveedores varían de un proveedor a otro. Algunos solo informan sobre el historial de acceso al *internet protocol* (protocolo de *internet*, o IP), otros informan sobre datos de geolocalización, hay empresas que proporcionan los puertos lógicos de origen asociados a las IPs, etc. Lo que importa es que, cuando los datos se obtengan por orden judicial, será posible delimitar la autoría de los delitos cibernéticos.

Sin embargo, esto requiere un análisis amplio y minucioso de los datos obtenidos por los agentes de la Policía Civil y la Policía Federal.

Saber más

El estudio de los datos proporcionados por los principales proveedores de aplicaciones de *internet* y los principales proveedores de conexión queda fuera del alcance de este curso teórico y exige un curso separado y más profundo.

Por este motivo, es necesario que se emprendan iniciativas de capacitación, doctrina y estudio en el ámbito de la delincuencia cibernética, ya que el cumplimiento de las medidas cautelares utilizadas en el entorno cibernético requiere conocimientos específicos y una gran capacidad de análisis por parte de los agentes de policía.

Por ejemplo, en el caso de un delito de difusión de material pornográfico infantil mediante un perfil de Facebook, si interesa a la investigación de seguimiento obtener datos de registro de ese perfil, basta con una carta de las autoridades del Ministerio Público, la Policía Civil y la Policía Federal en la que se soliciten

esos datos. Así, si Facebook envía el historial de las IPs utilizadas por el autor, es posible llegar a qué cliente del servicio de internet cuya conexión se utilizó para acceder a ese perfil de Facebook. **Esto se hace en la etapa de análisis intenso de datos.**

Figura 18: Identificación del delincuente virtual mediante el análisis de los datos obtenidos. **Fuente:** Pixabay (2020).

Con la lista de IPs proporcionada por Facebook, se debe enviar una carta al concesionario de telefonía e *internet* (Net, Movistar, Claro, Tim, Tigo, etc.) solicitando los datos registrados del cliente al que ha distribuido estas IPs. Esta carta debe hacer referencia a algunos datos. Podemos verlos en la imagen a continuación.

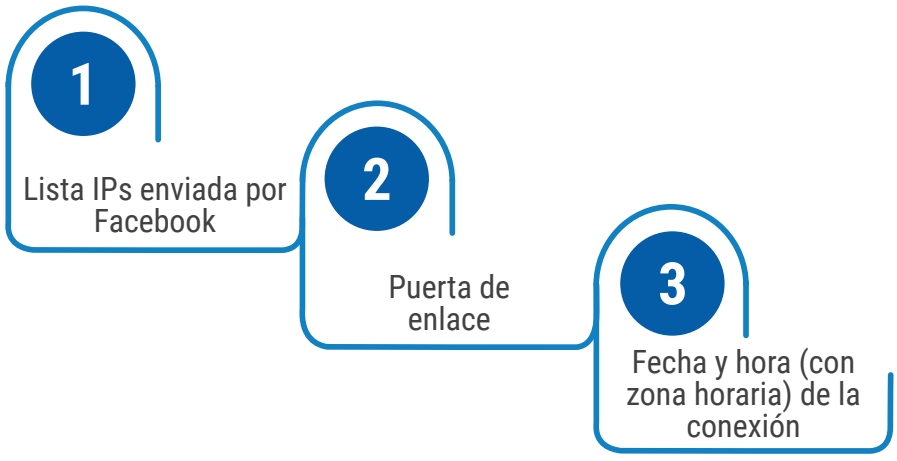


Figura 19: Datos que deberían incluirse en los oficios de los comerciantes de telefonía e *internet*. **Fuente:** labSEAD-UFSC (2020).

A partir de ese momento, el operador de telefonía e *internet* informará los datos de registro (incluida la dirección) del cliente al que distribuyó la IP en esa fecha y hora. En posesión de la dirección asociada a la conexión a *internet*, desde la que

se cometió el delito, el Ministerio Público, la Policía Civil y la Policía Federal pueden representar al Poder Judicial mediante la emisión de una orden de **búsqueda y aprehensión** a la dirección involucrada, con una solicitud de autorización para acceder a los datos y archivos. Aquí es donde se **dirige la investigación en el entorno cibernético.**

> De hecho, es en el cumplimiento de una eventual orden de registro e incautación que se revelará efectivamente la materialidad del delito y su autoría.

Con la aprobación de la orden de búsqueda y aprehensión, el Ministerio Público, la Policía Civil y la Policía Federal pueden localizar e incautar los dispositivos electrónicos en la dirección obtenida y someterlos a un **examen pericial**, que generará informes periciales en los que se analizará el contenido de dichos dispositivos y, eventualmente, se identificarán los **vestigios** del delito investigado.

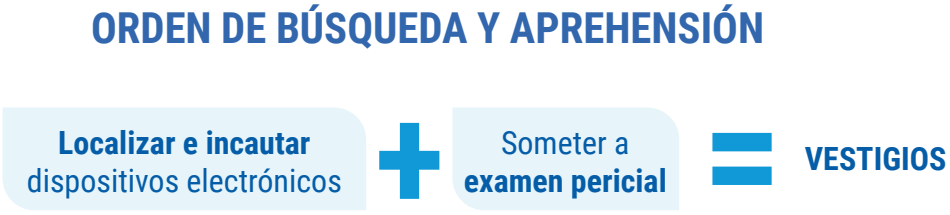


Figura 20: Proceso de búsqueda y aprehensión.
Fuente: labSEAD-UFSC (2020).

Paralelamente, la búsqueda y aprehensión permiten identificar a las personas que utilizan el sitio, lo que permite hacer preguntas a los involucrados. Incluso para el suscriptor de la conexión a *internet* existente en el sitio, estas respuestas suelen arrojar mucha información sobre la identificación de la autoría de los delitos.

Los procedimientos que se adopten en estos casos dependen de un curso práctico de la investigación del delito, pero hay que tener en cuenta que todos estos instrumentos (oficios, representaciones por orden judicial, etc.) utilizados en la

investigación de seguimiento permiten configurar la materialidad del delito investigado y llegar a la autoría de los delitos.

Por lo tanto, llegamos al final de otro módulo. Aquí conocimos, a través de la base teórica y jurídica, los aspectos generales de la investigación policial y los aspectos específicos de la investigación de los delitos electrónicos.

En la continuación del curso, comprenderemos que todos estos pasos que conforman la **investigación preliminar** y la **investigación de seguimiento** se aplicarán a un caso específico para que haya una mejor comprensión de la teoría que aquí se presenta. **¡Sigamos adelante!**

Referencias

BARRETO, A. G.; BRASIL, B. S. **Manual de investigação cibernética:** à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 15 jul. 2020.

BRASIL. **Decreto n.º 99.710, de 21 de novembro de 1990.** Promulga a Convenção sobre os Direitos da Criança. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 30 jul. 2020.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 8.137, de 27 de dezembro de 1990.** Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em: 30 jul. 2020.

BRASIL. **Lei n.º 10.446, de 8 de maio de 2002.** Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1º do art. 144 da Constituição. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10446.htm. Acesso em: 30 jul. 2020.

BRASIL. **Lei n.º 12.830, de 20 de junho de 2013.** Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 13.260, de 16 de março de 2016.** Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 31 jul. 2020.

BRASIL. Supremo Tribunal de Justiça. **Conflito de Competência 111.338-TO.** Relator: Ministro OG Fernandes, 23 jun. 2010. Brasília, DF, 1º jul. 2010. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/15026530/conflito-de-competencia-cc-111338-to-2010-0061596-0/inteiro-teor-15026531. Acesso em: 20 jul. 2020.

BRASIL. Supremo Tribunal de Justiça. Conflito de Competência 99.133-SP. Relator: Ministro Napoleão Nunes Maia Filho. **Diário de Justiça Eletrônico,** Brasília, DF, 19 dez. 2010.

FLATICON. [*S.l.*], 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 16 jul. 2020.

JORGE, H. V. N. **Investigação criminal tecnológica.** Rio de Janeiro: Brasport, 2018. 2 v.

PIXABAY. [*S.l.*], 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 16 jul. 2020.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 14 jul. 2020.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

MÓDULO 6

CASO CONCRETO DE INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN BRASIL

Presentación

En módulos anteriores, adquirimos nociones del espacio virtual e Internet, así como el aprendizaje de conceptos y características del delito cibernético, procedimientos virtuales de investigación y legislación sobre delitos cibernéticos.

A partir de ahora, trataremos un caso específico de investigación. Conoceremos un verdadero proceso digital de investigación criminal, que articulará el conocimiento expuesto en todos los módulos anteriores.

OBJETIVOS DEL MÓDULO

Conocer en detalle un proceso de investigación penal cibernética que ocurrió en Brasil.

ESTRUCTURA DEL MÓDULO

- **Clase 1 –** Lecciones Prácticas en la Investigación de los Delitos Cibernéticos.
- **Clase 2 –** Estructura de los Documentos Utilizados en la Investigación de Delitos Cibernéticos.

Clase 1 – Lecciones Prácticas en la Investigación de los Delitos Cibernéticos

CONTEXTUALIZANDO...

Antes de entrar en el caso específico de investigación de un delito cibernético, es necesario presentar una visión general del tema relacionado con esta investigación.

Es por este sesgo que ahora procederemos al estudio de las lecciones prácticas del proceso de investigación de crímenes digitales.

CASOS PRÁCTICOS: DELITOS CONTRA EL HONOR Y DELITOS CIBERNÉTICOS

Resumen histórico

En los últimos años se han adoptado una serie de nuevas prácticas relacionadas con las tecnologías modernas de comunicación actuales. En este contexto, uno de estos fenómenos es el *sexting*, término en Inglés que originalmente se refería al envío de mensajes de texto de naturaleza sexual, pero que, con el avance de los teléfonos móviles, comenzó a referirse a la práctica de enviar imágenes íntimas o videos (*nudes*, por ejemplo) por medio de teléfonos inteligentes u otros dispositivos electrónicos.

Saber más

El "*sexting*" aparentemente fue utilizado por primera vez en 2004 para referirse a mensajes intercambiados entre el jugador David Beckham y un asistente.

Un estudio de 2012, cuyo objeto era un grupo de personas de 18 años, indicó que el 30% de ellos ya habían enviado imágenes/videos íntimos a otra persona. La amplitud de este

fenómeno hace del *sexting* un campo fértil para la práctica de delitos, especialmente los delitos contra el honor, la extorsión y la violación. La práctica de extorsión y violación, a partir del *sexting*, constituye el objeto de la investigación que veremos a continuación.

En particular, en la investigación que se presentará, **el autor se hizo pasar por una mujer** en aplicaciones de redes sociales, en las que contactó a otras mujeres y niñas y les envió vídeos y fotos íntimas de la mujer por la que se hacía pasar. Cuando recibieron tales videos, las mujeres se sentían seguras de enviarle videos íntimos.

Figura 1: Cuando recibes o envías sexting, le das a otros la libertad para usarlas o compartirlas de la manera que les plazca. **Fuente:** Pixabay (2020).

En posesión de los vídeos íntimos, el autor amenazó con publicarlos, exigió dinero a las víctimas (extorsión), o les exigió que le enviaran fotos/vídeos en los que se masturbaran o introdujeran objetos en el ano o la cavidad vaginal (delito de violación).

De los hechos investigados

La investigación, utilizada aquí como un caso de aprendizaje, consistió en una investigación policial iniciada por la Policía

Civil del Distrito Federal para conocer las comunicaciones realizadas por las víctimas que denunciaron que una persona desconocida, que se hacía pasar por una mujer en redes sociales y aplicaciones, en particular, Snapchat y Tinder, actuó de tal manera para ganar la confianza de la víctima y luego cometer el crimen. La siguiente imagen muestra la forma de actuar del criminal:

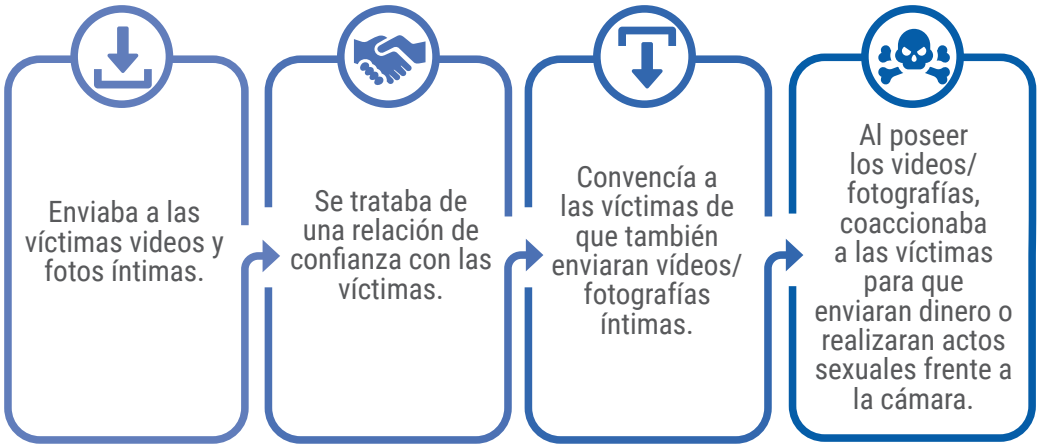


Figura 2: Acciones del autor del delito cibernético.
Fuente: labSEAD-UFSC (2020).

Estos comportamientos que acabamos de ver en la imagen anterior variaron según la víctima, pero vale la pena considerar que este no es un modus operandi nuevo.

¡Veamos otro ejemplo de un caso similar a continuación!

Estudio de Caso

Nicholas Glenn Wilcox creó un perfil falso de Facebook, en el que fingió ser una niña de 15 años y comenzó a comunicarse con un niño de 16 años. Durante las conversaciones, Wilcox envió fotos íntimas de una chica que el niño creía que era la chica con la que hablaba. A cambio, Wilcox pidió algunas fotos íntimas del niño. En posesión de estas fotos y bajo amenazas de publicarlas, Wilcox exigió que el niño introdujera un cepillo de dientes en su ano, se masturbase ante una cámara y le enviara fotos/videos de tales actos.

Tenemos otro ejemplo, donde analizaremos el crimen que empezamos en esta clase. A partir de ahora, conoceremos los informes de algunas de las víctimas de este crimen.

VÍCTIMA 1

La **VÍCTIMA 1** narró que comenzó a mantener contacto con un usuario de la aplicación Snapchat que usó como nombre de usuario "gabsgabs599" y se identificó como "Gabriela". La víctima le envió al usuario gabsgabs599 algunas fotos íntimas y videos.

Con el paso del tiempo, el usuario gabsgabs599 reveló a VÍCTIMA 1 que había guardado las fotos íntimas y videos que había subido y que conocía el perfil de Facebook de la víctima, así como su lista de amigos de esa red social. Luego comenzó a amenazarla, afirmando que, si ella no hacía todo lo que él exigía, le enviaría los archivos a sus amigos.

La VÍCTIMA 1 reportó que el usuario gabsgabs599 utilizó los siguientes términos, presentados en la siguiente imagen.

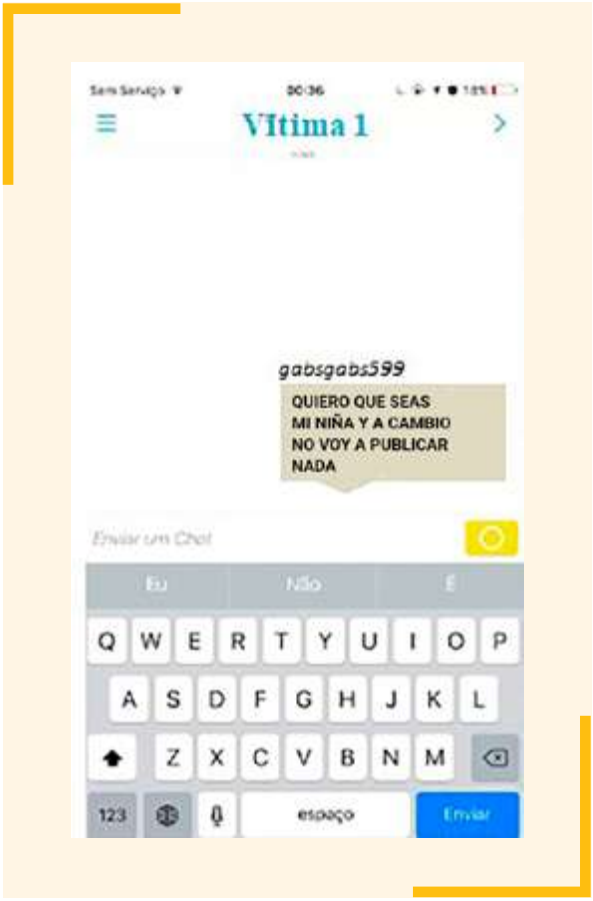


Figura 3: Amenaza del autor del crimen a la VÍCTIMA 1.
Fuente: Snapchat (2020), adaptado por labSEAD-UFSC (2020).

Así que el perpetrador, a través de las amenazas de divulgar las fotos y videos íntimos del declarante, exigió que produjera videos según sus peticiones. Ante estas amenazas, la VÍCTIMA 1 desactivó su perfil en la red social Facebook y dejó de coincidir con "Gabriela".

La VÍCTIMA 1 informó además que el desconocido había creado una cuenta *fake* (falsa) en la aplicación de Instagram (perfil de usuario @jajanoculm) y le envío una solicitud de amigo. En dicha solicitud, la víctima se dio cuenta de que en el perfil había las siguientes palabras: "CIERRA EL TRATO, NO HE BORRADO NADA." Consulta la captura de pantalla del perfil en la siguiente imagen.

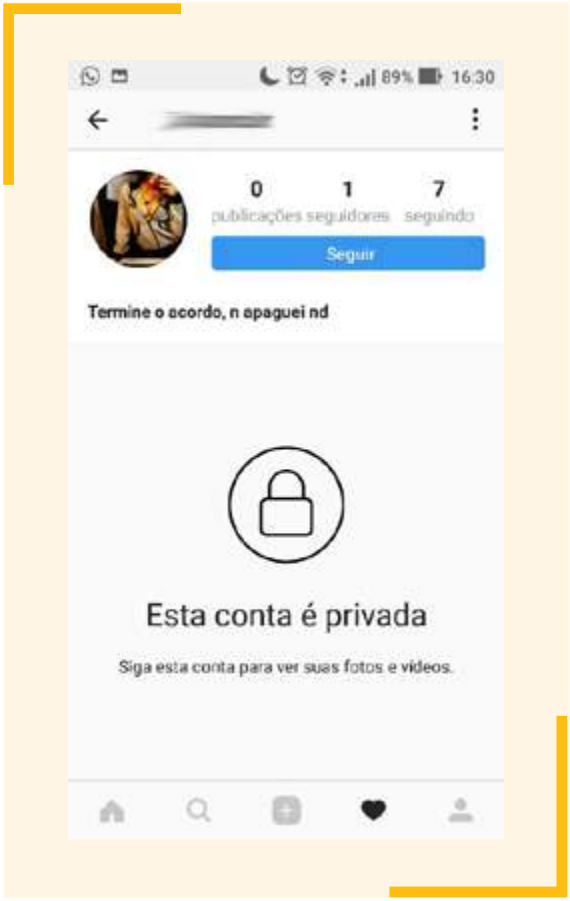


Figura 4: Captura de pantalla de Instagram proporcionada por VÍCTIMA 1. **Fuente:** EaD/SEGEN (2020), adaptado por labSEAD-UFSC (2020).

Continuemos nuestro análisis para conocer a la VÍCTIMA 2.

VÍCTIMA 2

La **VÍCTIMA 2** comentó que conoció a una persona llamada "Gabrielle" a través de la aplicación Tinder, quien le pidió que siguieran conversando a través de la aplicación Snapchat. En esta aplicación, la VÍCTIMA 2 señaló que "Gabrielle" usaba el nombre usuario "gabsgabs599". A partir de una solicitud, la VÍCTIMA 2 le envió a "Gabrielle" algunas fotos y videos sin ropa, ya que se sentía en una relación de confianza.

En un momento dado, el usuario "gabsgabs599" reveló que tenía las fotos y vídeos íntimos que la VÍCTIMA 2 había enviado y que conocía su perfil de Facebook, así como su lista de amigos de esa red social. A la luz de esto, el autor informó que, si ella no le enviaba una suma de 1.500 reales, él vendería las fotos/videos a un sitio *web*, así como enviaría esos archivos a sus amigos de Facebook.

Figura 5: Amenaza del autor a la VÍCTIMA 2. **Fuente:** labSEAD-UFSC (2020).

El Usuario "gabsgabs599" le pidió a la VÍCTIMA 2 que facilitara su dirección de *email*, para enviarle una solicitud de cobro a través de la aplicación PayPal, pero la VÍCTIMA 2 no cedió y fue a la Policía Civil del Distrito Federal para presentar una denuncia sobre los hechos.

VÍCTIMA 3

La **VÍCTIMA 3**, menor de edad, informó que había estado en contacto en *internet* con una persona identificada como "Gabrielle" ("Gabi"). El contacto inicial fue por la aplicación Tinder y luego continuó con la aplicación Snapchat (usuario "gabsgabs599" y más tarde "gpont10"). Observa la siguiente imagen:

Figura 6: Captura de pantalla con el cambio de nombre de usuario del autor con la VÍCTIMA 3. **Fuente:** EaD/SEGEN (2020), adaptado por labSEAD-UFSC (2020).

Cabe destacar que “Gabi” le preguntó la edad a la VÍCTIMA 3 por solicitud de Snapchat, y ella informó que tenía 16 años. En un momento dado, Gabi le envió a la VÍCTIMA 3 una foto supuestamente posando desnuda. Acto seguido, “Gabi” le pidió a la VÍCTIMA 3 que hiciera lo mismo, es decir, enviarle una foto desnuda. Más tarde, “Gabi” le pidió a la VÍCTIMA 3 que enviara una foto desnuda donde fuese posible ver su cara, lo cual hizo.

En un día determinado, cuando accedió a la red de su casa, la VÍCTIMA 3 verificó en su Snapchat que “Gabi” había dejado varios mensajes amenazantes sobre que publicaría todas sus imágenes en las redes sociales, principalmente, a su familia y amigos, a quienes **citó nominalmente.**

Ante una grave amenaza, sobre todo porque “Gabi” afirmó que lo había hecho en otras ocasiones y que nunca había sido descubierta, la VÍCTIMA 3 decidió satisfacer las demandas, pero también decidió grabar todas las conversaciones. “Gabi” dijo que la VÍCTIMA 3 debía obedecerla durante tres meses, atendiendo a sus demandas sexuales, tiempo durante el cual mantendría sus archivos almacenados y luego los borraría.

En estas conversaciones, por ejemplo, el perpetrador del crimen dijo que la VÍCTIMA 3 debería ser “mi pequeña zorra por algún tiempo [...] dándome placer” y exigió algunas acciones de la VÍCTIMA 3: abrir la boca, sacar la lengua y dejar que la saliva escurriese por la lengua, recoger “algo grande y grueso” o “un cepillo para el cabello” o un “desodorante” o un “champú” e introducirlos “dentro de su vagina”, masturbarse, introducir “2 dedos” y “luego 3 dedos” en la vagina, “chupar” un desodorante y colocar lubricante en la vagina.

La VÍCTIMA 3 decidió satisfacer las demandas y fue al baño y comenzó a hacer todo lo requerido por el autor del crimen. Así que insertó objetos como un rímel en la cavidad vaginal, lamió el objeto, insertó sus dedos en la cavidad vaginal, mostró a la cámara su vagina y el ano, e hizo poses sexies delante de la cámara.

Después de que la víctima cumpliera casi todo lo que se le requería, el autor dijo que era suficiente para ese día y que volvería más tarde. Al temer lo que pudiera suceder, la VÍCTIMA 3 le contó los hechos superficialmente a su madre y asistió a la Policía Civil del Distrito Federal para registrar el incidente policial.

VÍCTIMA 4

La **VÍCTIMA 4**, menor de edad, informó que cuando utilizaba la aplicación Snapchat, recibió una solicitud de amigo del usuario "gpont10", que utilizaba el nombre "Gabs". La VÍCTIMA 4 aceptó la solicitud y empezó a hablar con ella. En las conversaciones, "Gabs" preguntó de dónde era la VÍCTIMA 4, qué hacía y qué edad tenía, así como otras preguntas similares.

Sobre la edad, la VÍCTIMA 4 señala que informó que tenía 17 años, a lo que "Gabs" respondió que también tenía esa edad. Unos días más tarde, "Gabs" le envió a la víctima varias fotos y propuso que ambas intercambiaran fotos usando solo un sujetador. "Gabs" luego envió una foto con un sujetador.

A partir de esto, la VÍCTIMA 4, sintiéndose segura de que recibió la foto, también le envió una foto suya usando un sujetador. Posteriormente, "Gabs" envió una foto desnuda de la cintura para arriba. Del mismo modo, la VÍCTIMA 4, sintiéndose en una relación de confianza, también envió una imagen desnuda de sí misma desde la cintura para arriba.

Este *modus operandi* se repitió tanto que intercambiaron fotos con senos expuestos, para un total de entre cinco o siete fotos de esta naturaleza. Más tarde, "Gabs" envió una foto en la que aparecía su cara y le pidió a la VÍCTIMA 4 que también enviara una foto de su cara, cosa que ella hizo.

En posesión de una foto en la que aparecía VÍTIMA 4 desnuda de la cintura para arriba y donde se podía ver su cara, el criminal informó: "Soy un bebé falso. Poco después, el autor envió una impresión de la página de Facebook de VICTIM 4 y dijo que sabía quiénes eran sus amigos y que si no le pagaba en media hora, empezaría a publicar las fotos, y "Gabs" empezó a declinar varios nombres de amigos de VICTIM 4.

Figura 7: Amenaza del autor del crimen a la VÍCTIMA 4. **Fuente:** labSEAD-UFSC (2020).

La VÍCTIMA 4 señala que "Gabs" exigió la cantidad de R$ 1.000. Sin embargo, ella dijo que no tenía este valor, por lo que "Gabs" exigió solo R$ 200. Debido a la demora en el pago, "Gabs" cambió de parecer y le exigió R$ 400 la VÍCTIMA 4, así como también le exigió que realizara el pago a través del sitio *web* ***Portal dos Créditos,*** donde debía comprar dos gift cards de R$ 200.

A continuación, la VÍCTIMA 4 le dijo a Gabs que le contaría todo a sus padres e iría a la policía. El autor del crimen, en respuesta, dijo que no serviría de nada, porque estaba a 2.000 kilómetros de distancia de la víctima. Aun así, la VÍCTIMA 4, el 16/08/2017, se dirigió a la Policía Civil del Distrito Federal con sus padres, donde registró un informe policial.

VÍCTIMA 5

La **VÍCTIMA 5** aceptó una solicitud en la aplicación Tinder, procedente del usuario "Gabrielle Passos". Dos días más tarde, "Gabrielle" pidió ir a la aplicación Snapchat, en la que la VÍCTIMA 5 usaba el nombre "looh.raany" y "Gabrielle" usaba "gpont10".

En las conversaciones, "Gabrielle" sugirió divertirse intercambiando fotos íntimas y videos. Por lo tanto, "Gabrielle" le envió a la víctima varias fotos pornográficas y videos supuestamente de ella (en tales videos había incluso videos de "Gabrielle" supuestamente en los que introducía frascos en su vagina). Al sentirse en una relación de confianza, la VÍCTIMA 5 envió fotos suyas usando un sujetador. Más tarde, "Gabrielle" le pidió fotos desnudas que mostraran su rostro. La víctima le envió fotos de esta naturaleza.

Ante eso, "Gabrielle" dijo, "Soy un bebé falso". Poco después, "Gabrielle" amenazó con publicar las fotos y videos de VÍTIMA 5, exigiendo la cantidad de R$ 1.000,00 para no publicar dicho material. Sin embargo, dijo que no tenía esta cantidad y luego "Gabrielle" permitió que la cantidad se pagara en dos cuotas de R$ 500.00.

Figura 8: Amenaza del autor del crimen a la víctima 5.
Fuente: labSEAD-UFSC (2020).

Parte de las conversaciones se llevaron a cabo a través de la aplicación WhatsApp, asociado con el número de teléfono +1 (306) 700-XXXX. Con la intención de que la VÍCTIMA 5 realizara el pago, "Gabrielle" preguntó si tenía una tarjeta de crédito o una cuenta en el sistema *online* de transferencia de valores PayPal, pero la VÍCTIMA 5 dijo que no. Por lo tanto, la VÍCTIMA 5 decidió no pagar e ir a la policía para denunciar los hechos.

Ahora que tenemos conocimiento de los casos en los que un criminal se hacía pasar por alguien llamado "Gabrielle" en un perfil falso, entenderemos el proceso de investigación después de la denuncia de las víctimas.

Procedimientos de investigación

Después de los informes de las víctimas, debe iniciarse la investigación preliminar del delito, que, como se muestra, en el caso de los delitos cibernéticos, busca lograr ciertos fines.

Observa la siguiente imagen y recuerda los propósitos preliminares de una investigación de delitos cibernéticos.

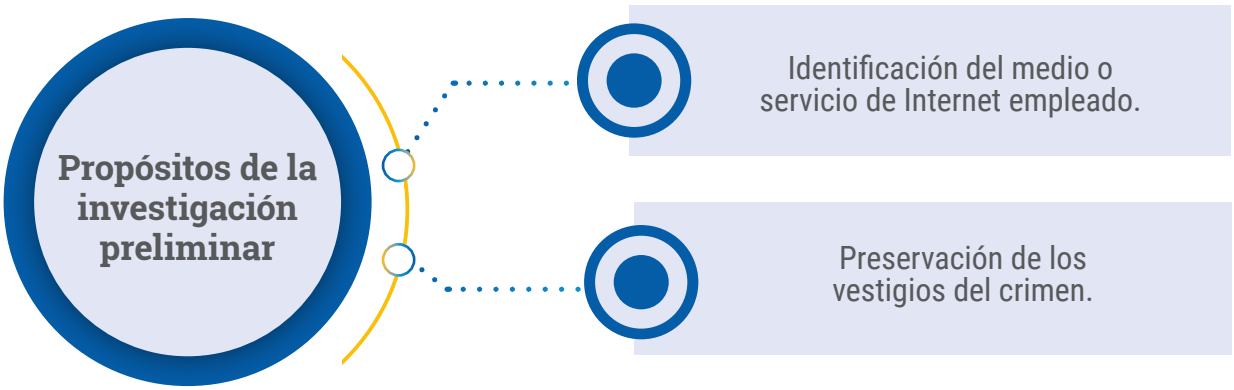


Figura 9: Propósitos de la investigación preliminar del delito cibernético.
Fuente: labSEAD-UFSC (2020).

En cuanto al medio o servicio de *internet* empleado para la práctica de los crímenes narrados, no hay problemas importantes. En la narración de las propias víctimas, es posible verificar que los delitos se cometieron a través de las redes sociales involucradas (Snapchat, Tinder e Instagram).

El siguiente paso en la investigación preliminar es entonces la preservación de los vestigios del crimen, que presenta dos etapas, que se pueden identificar en la siguiente imagen.

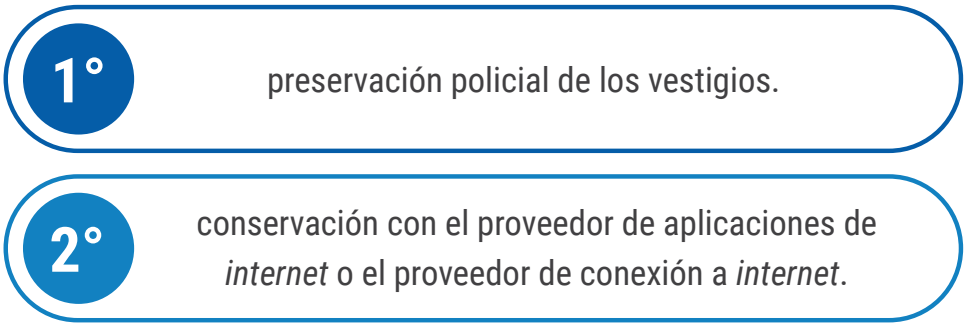


Figura 10: Pasos de preservación de vestigios en la investigación de delitos digitales. **Fuente:** labSEAD-UFSC (2020).

En lo que se refiere al caso de las víctimas de "Gabrielle", la preservación policial de los vestigios se hizo a través de un certificado policial asociado con *print screen* (captura de pantalla) de las imágenes o escritos que comprueban los crímenes aquí investigados. A continuación, se llevó a cabo la preservación de datos con los proveedores de aplicaciones de Internet. En este caso, se buscó la preservación de los datos asociados a los perfiles de las redes sociales involucradas (Snapchat, Tinder e Instagram) que entraron en contacto con las víctimas.

En el siguiente paso, los agentes de policía prepararon un **informe** de investigación que contenía todo lo que se había hecho y recogido en la investigación preliminar. Este informe fue luego **enviado al delegado de la policía** que presidía la investigación para facilitar la **toma de decisiones**. A partir del informe, el delegado le dio inicio a la investigación de seguimiento y le solicitó al Poder Judicial la eliminación del sigilo de los datos telemáticos de las cuentas de las redes sociales involucradas (Snapchat, Tinder e Instagram), el cual fue diferido. Pero vale la pena señalar que las solicitudes a

Snapchat y Tinder tienen sede legal en los Estados Unidos de América (EE.UU.), por lo tanto están fuera del alcance de la jurisdicción del Poder Judicial Nacional brasilero.

Saber más

En el caso de los Estados Unidos, cabe destacar el Acuerdo de Asistencia Judicial Mutua en Materia Penal (MLAT) firmado entre el Gobierno de la República Federativa del Brasil y el Gobierno de los Estados Unidos de América. De esta manera, la orden de eliminación del sigilo podría enviarse a los Estados Unidos a través del MLAT.

Puedes entender más acerca de este Acuerdo al hacer clic en el *link* a continuación.

Decreto n.º 3.810, de 2 de maio de 2001 - http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm

De igual forma, Instagram señaló varias direcciones IP utilizadas para acceder a la cuenta investigada "@jajanoculm" con los datos de fecha, hora y zona horaria de acceso. Por ejemplo, una de las IP reportadas por Instagram era la dirección IP 181. XXX.156.YY, que pertenece al conjunto de IPs de Claro S.A.

En posesión de estos datos, el delegado policial que presidió la investigación solicitó a la empresa Claro S.A. los datos de registro del cliente que utilizó dicha propiedad intelectual. El operador informó que la IP, en la fecha, hora y zona horaria informada, se distribuyó al cliente A.J.B.N., residente en la dirección X y en la ciudad de Nova Parnamirim en el estado de Río Grande del Norte.

Con el fin de analizar esta información, los agentes de policía prepararon otro informe de investigación en el que se centralizaron los datos recopilados hasta el momento y se señalaron los nuevos datos obtenidos, como los residentes de la ubicación antes mencionada, a saber:

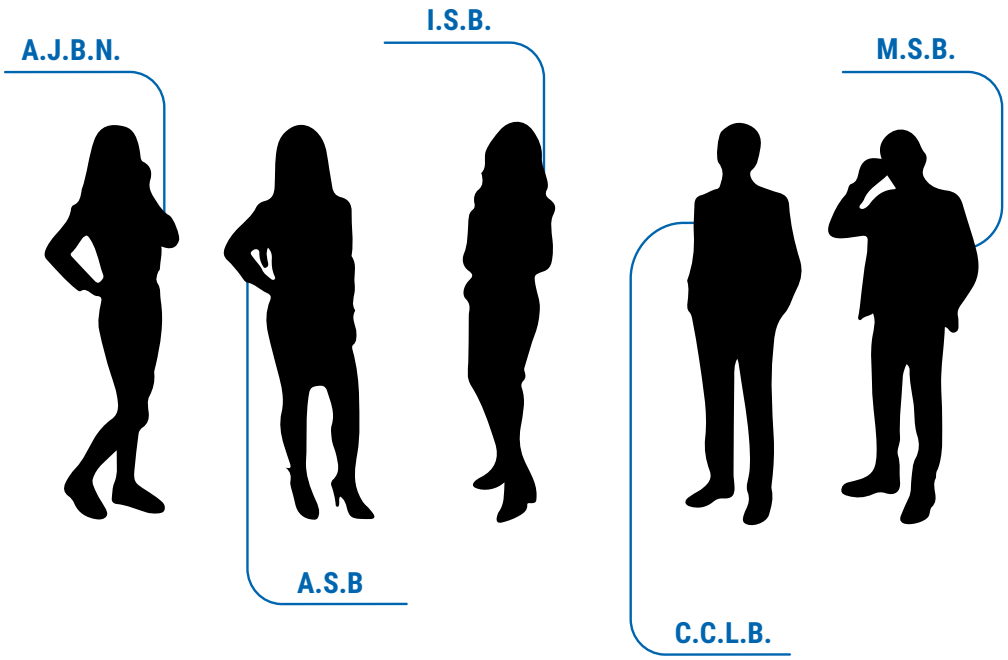


Figura 11: Datos de los residentes de la ubicación. **Fuente:** labSEAD-UFSC (2020).

Al continuar la investigación, los delegados presentaron el registro e incautación en esa dirección, que fue otorgado por el Poder Judicial. De esta forma, con la orden de allanamiento e incautación, un equipo de la Policía Civil del Distrito Federal (PC/DF), compuesto por agentes de policía responsables de la investigación, un experto criminal y el delegado, se dirigió a la ciudad de Nova Parnamirim/Río Grande del Norte, para cumplir con dicha orden de registro e incautación en la dirección obtenida.

Durante la búsqueda, el equipo verificó a los residentes presentes A.J.B.N., A.S.B., I.S.B., C.C.L.B. y M.S.B., de los cuales se recogieron declaraciones. Con M.S.B., el experto comprobó varios elementos que indicaban que él era el autor de los delitos investigados, ya que el dispositivo tenía una aplicación emuladora del sistema operativo Android, en la que inicialmente se localizaron alrededor 4200 archivos de vídeos y fotos pornográficos, incluidos archivos relativos a las víctimas de la investigación.

> Al final de las declaraciones recogidas tras el registro y la incautación, M.S.B. proporcionó información que, junto con los elementos obtenidos en el registro y la incautación, daban razones fundadas de que él era el autor de los delitos investigados en esta investigación.

Debido al material encontrado en su computadora, que configuró el delito del artículo 241-B del Estatuto de la Niñez y la Adolescencia — tienda de fotografía, video u otra forma de registro que contenga una escena sexual explícita o pornográfica que involucra a niños o adolescentes — M.S.B. fue detenido por la Policía Civil del Distrito Federal.

Más tarde, el informe forense criminal indicó que en la computadora analizada se instaló el sistema operativo Windows, que sólo tenía un usuario activo llamado M.B.O. El experto criminal también identificó que otras aplicaciones se instalaron en el disco duro del dispositivo, que se describen en la siguiente imagen.

1. **Bluestacks:**
   destinado a emular un ambiente con sistema operativo Android.
2. **Hushed:**
   permitía el uso de números telefónicos temporales vinculados a un país, lo que permitía, por ejemplo, el anonimato en las llamadas.
3. **Casper:**
   tiene la función de burlar los sistemas de seguridad de la aplicación Snapchat, lo que permite grabar las imágenes y videos publicados por otros usuarios sin el conocimiento de quien realizó la publicación.
4. **Instagram:**
   a pesar de que estaba instalada, no se encontraba en uso.

5 **Drive:**

en esta aplicación se encontraron 5.603 videos e imágenes, también casi en su totalidad involucraban mujeres en escenas pornográficas y con nombres de archivo que señalaban los usuarios que los enviaron.

6 **QuickPic:**

se utiliza para agrupar y facilitar la visualización de imágenes y videos, donde se localizaron 4.210 videos e imágenes, en donde casi todos involucraban mujeres en escenas pornográficas, divididos en categorías como “savedSnaps”, “snapchat”, “whatsappimages” y “whatsappvideos”, así como también con nombres vinculados a los usuarios que los enviaron.

7 **Snapchat:**

se encontraba configurada para el usuario “gpassos101” y presentaba 43 usuarios en la lista de contactos.”

8 **Tinder:**

estaba configurada para el usuario de nombre GABS, con interés exclusivo en mujeres entre las edades de 18 (edad mínima permitida por la aplicación) y 27 años. El perfil se autoidentificaba como “bi”, “17 años” y “buscando diversión en snap y con quien salir dependiendo de lo que suceda”. Vale la pena destacar que en las conversaciones identificadas, el usuario GABS sugería el uso de la aplicación Snapchat para intercambiar fotos y videos con contenido sexual.

9 **WhatsApp:**

se encontraba configurada para el número telefónico +1(306)700-XXXX (uno de los números encontrados en la aplicación Hushed) y presentaba el nombre de usuario GABS. De igual forma, en algunos de los ocho registros de conversaciones recuperados, se podía observar al usuario “Gabs” amenzando con divulgar material pornográfico producido por las víctimas, en caso de que éstas no produjeran nuevos videos o imágenes pornográficas o efectuaran la transferencia de valores.

10 **PayPal:**

finalmente, la investigación identificó registros en el sitio web PayPal, destinados al envío y recibimiento online de pagos, donde se evidenciaba varios movimientos financieros del usuario M.S.B.

Figura 12: Aplicaciones encontradas en el dispositivo utilizado por el delincuente para practicar el delito. **Fuente:** labSEAD-UFSC (2020).

Tras el análisis de los archivos encontrados en el ordenador, el equipo de la PC/DF llegó a algunas conclusiones, que identificamos en la siguiente imagen.

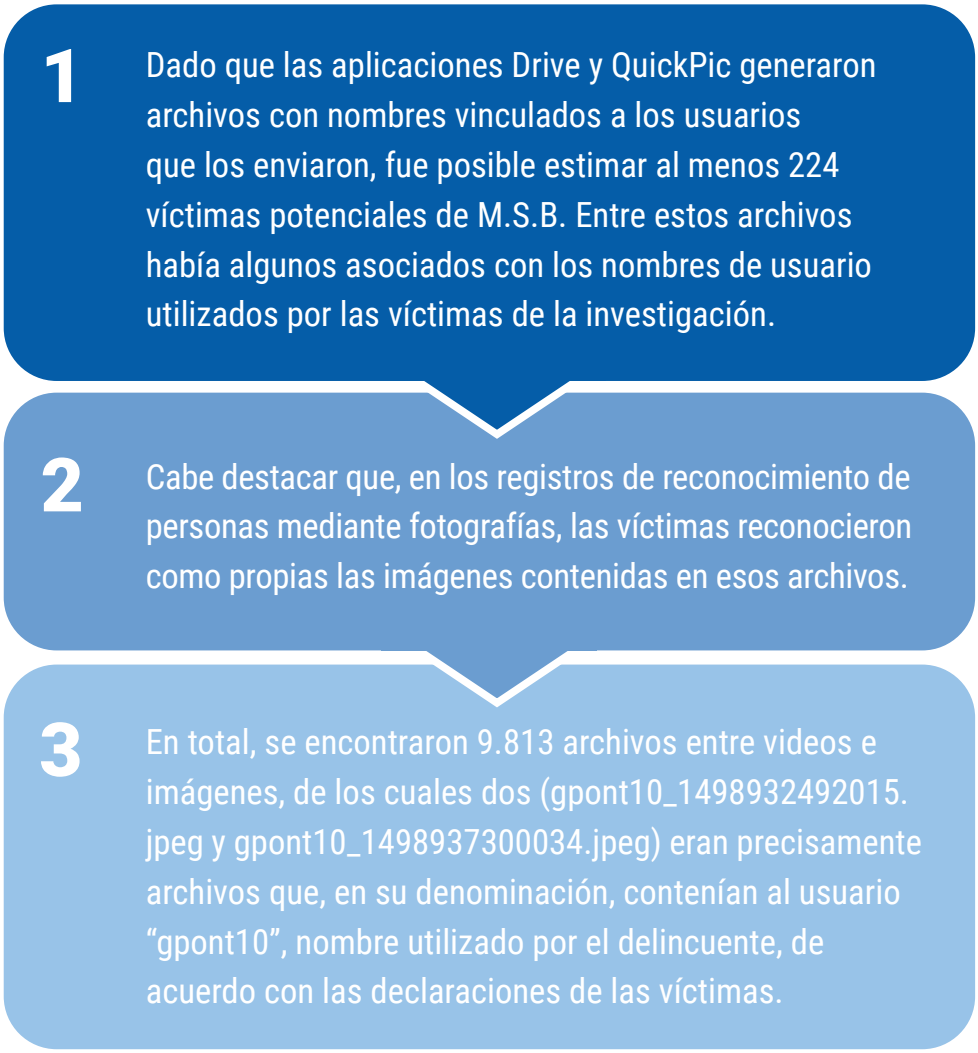


Figura 13: Conclusiones planteadas por el equipo de investigación del delito en cuestión. **Fuente:** labSEAD-UFSC (2020).

Es decir, se encontraron pruebas suficientes para concluir con seguridad que la computadora de M.S.B. tenía vestigios que afirmaban ser el usuario de los perfiles "gabsgabs599" y "gpont10", denunciados por las víctimas. Ante todo esto, M.S.B. fue acusado por el delegado por algunos crímenes.

A continuación se mencionan dichos crímenes:

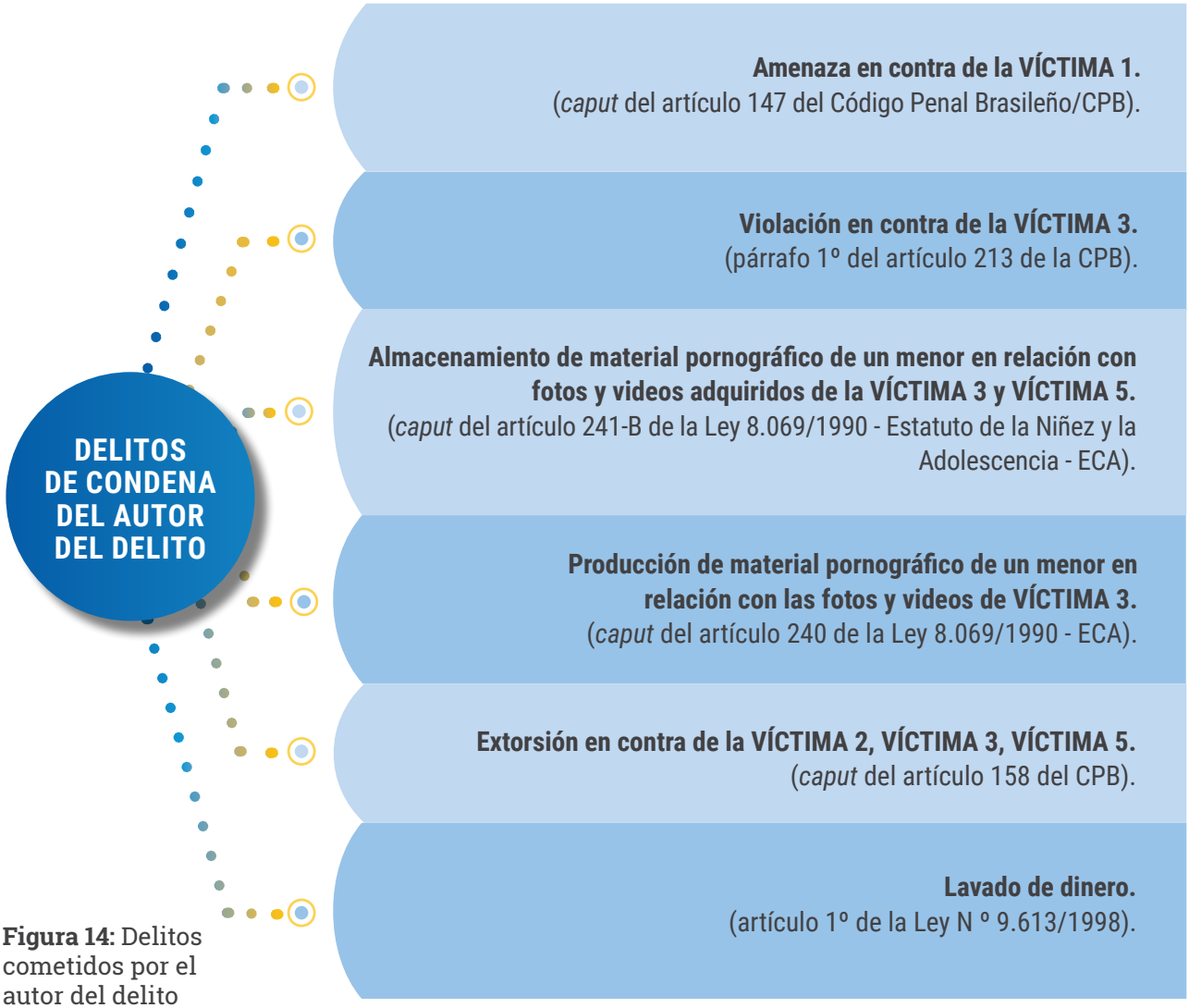


Figura 14: Delitos cometidos por el autor del delito contra el que fue acusado. **Fuente:** labSEAD-UFSC (2020).

Sobre el lavado de dinero que observamos como el último tema de la Imagen anterior, es necesario entender que M.S.B. extorsionó a algunas víctimas y les obligó a transferir dinero a una cuenta en un sitio *web*. Este *site* tiene como objetivo la venta de créditos y tarjetas de juegos. En estos casos, la compra de créditos se realiza por medio de transferencia de valores.

Los usuarios de juegos *online* utilizan este *site* para comprar artículos virtuales para los juegos de su elección. Por lo tanto, M.S.B., como una forma de obtener una ventaja económica ilícita, obligó a las víctimas de la extorsión a que le compraran créditos en la plataforma, donde utilizaba el usuario “mexxxx”.

Una vez en posesión de dichos créditos, M.S.B. compraba objetos virtuales de la compañía de producción de juegos virtuales Steam, responsable del juego Counter-Strike. Vale la pena señalar que estos artículos son llaves para abrir cajas con objetos de juego. En posesión de estos artículos, el criminal los vendía a otros usuarios del juego Counter-Strike, en el *site* www.opskins.com, quienes pagaban por dichos artículos mediante la transferencia de valores a su cuenta en el sistema de transferencia electrónica de dinero PayPal. El gráfico a continuación resume este m*odus operandi*.

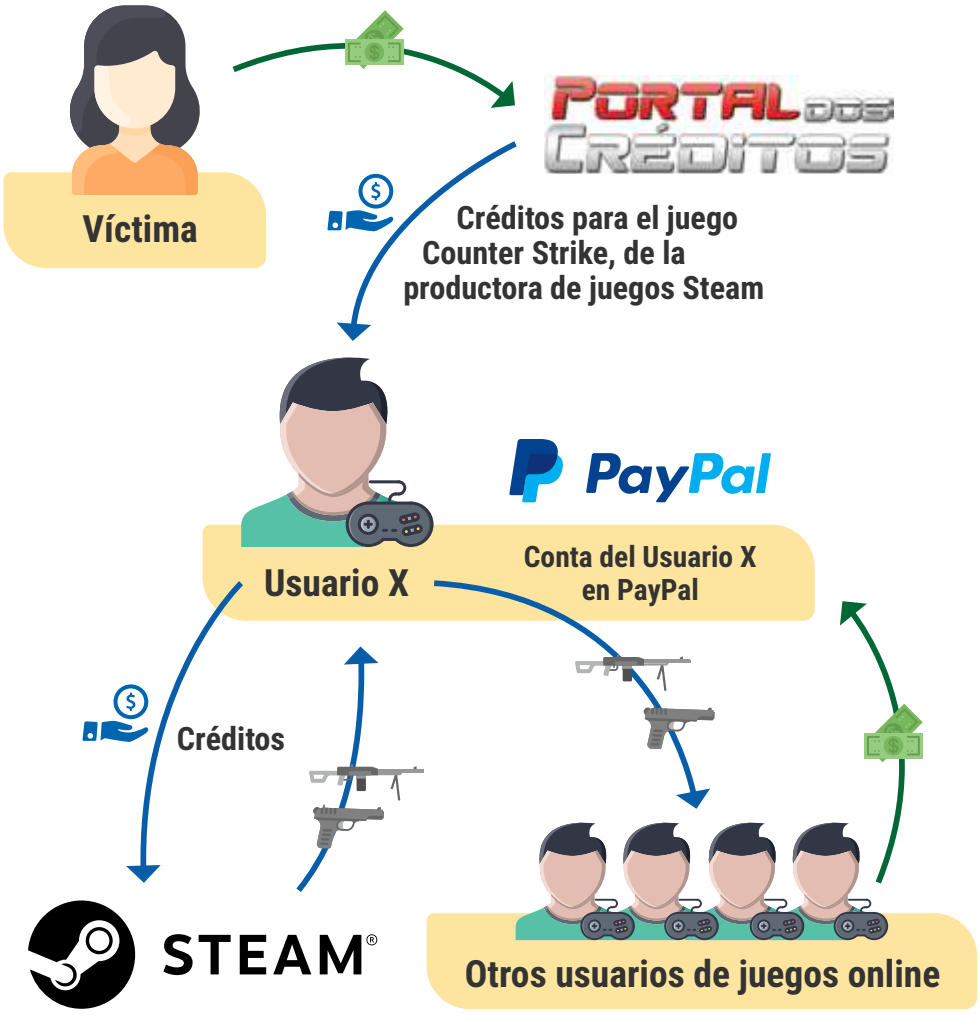
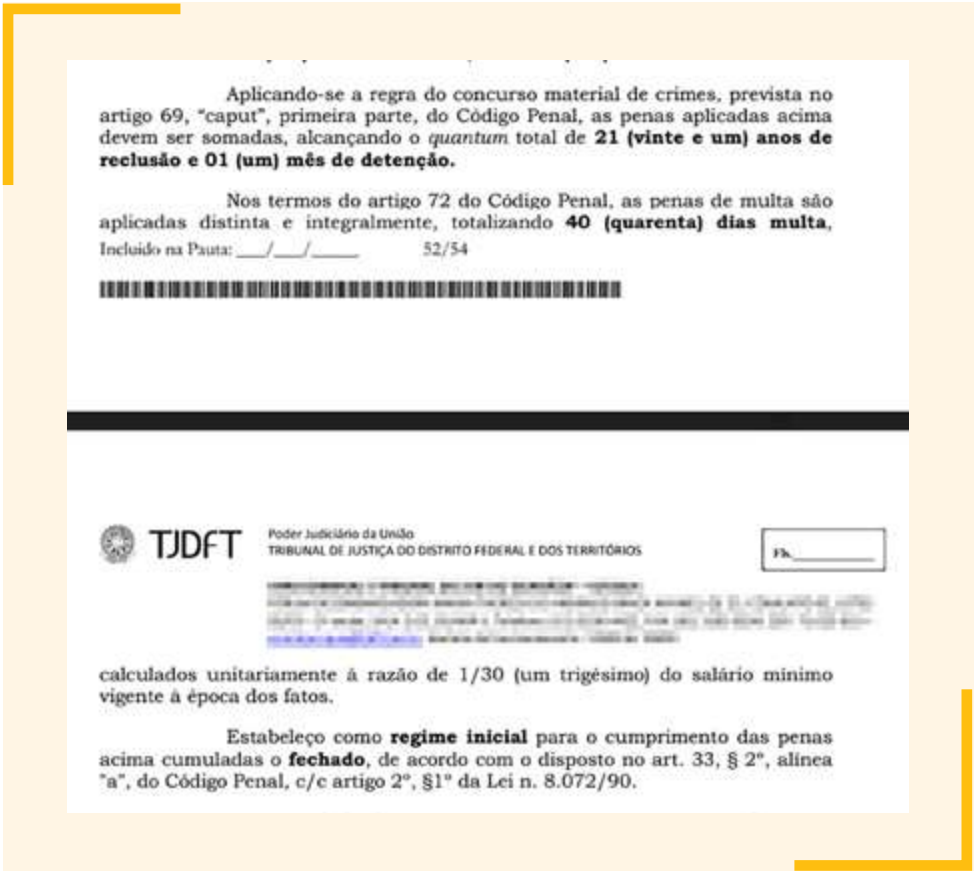


Figura 15: *Modus operandi* del criminal. **Fuente:** EaD/SEGEN (2020), adaptado por labSEAD-UFSC (2020).

De esta forma, las extorsiones que el criminal realizaba eran depositadas en su cuenta PayPal para la venta, aparentemente lícita, de objetos virtuales a los usuarios del juego *online*, que distanció esos fondos de su origen ilícito, para evitar de esta forma su asociación directa con los delitos de extorsión, lo que obstaculizó el rastreo de estos recursos y estableciendo **el delito de lavado de dinero.**

Después de la acusación, el delegado que presidió la investigación presentó al Poder Judicial la solicitud de convertir la prisión temporal de M.S.B. en prisión preventiva, pedido que fue aceptado. Posteriormente, M.S.B. fue denunciado por la Fiscalía del Distrito Federal y, al final del proceso penal, fue condenado por el Tribunal Federal de Justicia del Distrito a 21 años de prisión, 1 mes de detención y al pago de 40 días de multa fijada en 1/30 del salario mínimo en el tiempo de los hechos, como podemos identificar en la siguiente imagen.



Aplicando-se a regra do concurso material de crimes, prevista no artigo 69, "caput", primeira parte, do Código Penal, as penas aplicadas acima devem ser somadas, alcançando o *quantum* total de **21 (vinte e um) anos de reclusão e 01 (um) mês de detenção.**

Nos termos do artigo 72 do Código Penal, as penas de multa são aplicadas distinta e integralmente, totalizando **40 (quarenta) dias multa**, Incluído na Pauta: ___/___/_____ 52/54

[redacted]

TJDFT Poder Judiciário da União
TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS

Fls._____

[redacted]

calculados unitariamente à razão de 1/30 (um trigésimo) do salário mínimo vigente à época dos fatos.

Estabeleço como **regime inicial** para o cumprimento das penas acima cumuladas o **fechado**, de acordo com o disposto no art. 33, § 2°, alínea "a", do Código Penal, c/c artigo 2°, §1° da Lei n. 8.072/90.

Figura 16: Extracto de la sentencia condenatoria.
Fuente: EaD/SEGEN (2020).

Hasta ahora, conocemos el proceso de investigación de un caso específico de delitos cibernéticos. Continuemos con nuestros estudios y conozcamos un caso más de la práctica de crímenes virtuales y su proceso de investigación.

CASO PRÁCTICO: DIVULGACIÓN DE VÍDEOS ÍNTIMOS

Resumen histórico

Anteriormente, vimos que la conducta conocida como *revenge porn*, o "pornografía no consensual", se caracteriza como una transgresión de la intimidad de la mujer a través de la exposición no autorizada de sus imágenes íntimas y que se solía asumir como crimen de perjuicio, previsto en el artículo 140 del Código Penal brasileño (CPB).

> Sin embargo, a partir del 25/9/2018, gracias a la inclusión del artículo 218-C en el CPB por la Ley 13,718/2018, la práctica del *revenge porn* pasó a ser considerada autónomamente como causa del aumento del crimen de divulgación de escena de violación o de escena de violación vulnerable, de escena de sexo o de pornografía.

En otras palabras, el derecho penal brasileño llegó a prever específicamente como delito autónomo, en el artículo 218-C, la conducta de ofrecer, intercambiar, poner a disposición, transmitir, vender o exponer para la venta, distribuir, publicar o difundir, por cualquier medio, fotografía, video u otro disco audiovisual que contenga, sin consentimiento de la víctima, una escena sexual, desnudez o pornografía, siendo la pena (que es de reclusión, de 1 a 5 años) aumentada de 1/3 a 2/3 si el delito es cometido por una persona que mantiene o ha mantenido una relación íntima de afecto con la víctima o con el fin de venganza o humillación.

Por lo tanto, se convirtió en un delito autónomo, en la forma aumentada, por ejemplo, la conducta del ex novio que proporciona un video íntimo de la ex pareja con el propósito de venganza o humillación. En resumen, la conducta del *revenge porn* pasó a ser un crimen autónomo en Brasil. En este contexto, conoceremos el proceso de investigación de un caso real de la práctica de pornografía no consensuada.

De los hechos investigados

La investigación utilizada aquí como caso de aprendizaje consistió en una investigación policial iniciada por la Policía Civil del Distrito Federal para determinar la comunicación hecha por la víctima E.P.C., quien, en la comisaría de policía, reportó hechos vinculados a la íntima relación de afecto que mantuvo con G.A.S.

E.P.C. narró que salía con G.A.S. durante seis meses y que, a principios de noviembre de 2018, G.A.S. estaba en la residencia de E.P.C. cuando comenzó a mirar su teléfono celular. E.P.C., considerando que tenía un comportamiento muy posesivo, dejó claro que ya no quería la relación afectiva con él.

G.A.S., entonces, molesto por la declaración de E.P.C., la arrojó sobre la cama y, colocando su cuerpo sobre el suyo, gritó que "estarían bien" mientras la sacudía sobre el colchón, sin causarle aparentes lesiones corporales.

Figura 17: Agresión física por obsesión. **Fuente:** labSEAD-UFSC (2020).

E.P.C. añadió que le pidió a su novio que se detuviera, mientras comenzaba a llorar, cuando luego le escupió en la cara y dejó la propiedad, llevando consigo las llaves del vehículo y la residencia de E.P.C., las cuales sólo devolvió el 29/12/2018, a través de una orden enviada vía correo (Sedex). E.P.C. explicó que desde entonces, G.A.S. comenzó a hacerle varias llamadas telefónicas, llegando alrededor de 49 veces el mismo día.

Finalmente, E.P.C. informó que el 31 de diciembre de 2018, se enteró a través de su amigo B.C.B.G., que varias imágenes íntimas y videos de ella le habrían sido enviados (B.C.B.G) desde la terminal telefónica (61) 9XXXX-YYYY a través de la aplicación WhatsApp. Era sobre unas fotos en las que E.P.C. estaba desnuda y videos en los que se masturbó.

E.P.C. informó que, al ver las fotos y videos antes mencionados, se dio cuenta de que podrían haber sido enviados por G.A.S., ya que, según E.P.C., las imágenes y videos fueron hechos por su ex novio y ella misma, cuando todavía estaban juntos, aclarando que nadie más poseía tales archivos excepto ellos dos (G.A.S. y E.P.C.).

Procedimientos de investigación

En posesión del informe de la víctima, como hemos observado, se inicia la investigación preliminar del delito. En este sentido, identificamos que, en la propia narrativa de la víctima, es posible verificar que los crímenes se cometieron a través de la aplicación WhatsApp. El siguiente paso de la investigación preliminar es, entonces, la preservación de los vestigios, que se hizo a través de un certificado policial asociado con la descarga de imágenes y videos del amigo de la víctima B.C.B.G.

A continuación, se promovió la preservación de datos con el proveedor de aplicaciones de *internet*. En este caso, se promovió la preservación de los datos asociados con la cuenta de WhatsApp que contactó al amigo de la víctima B.C.B.G.

El siguiente paso fue la preparación del informe de investigación, que contenía todo lo que se hizo y planteó en la investigación preliminar. Este informe se envió luego al delegado de la policía que presidía la investigación para apoyar su toma de decisiones. Con el informe, el delegado inició la investigación de seguimiento. Veamos los procedimientos en la siguiente imagen.

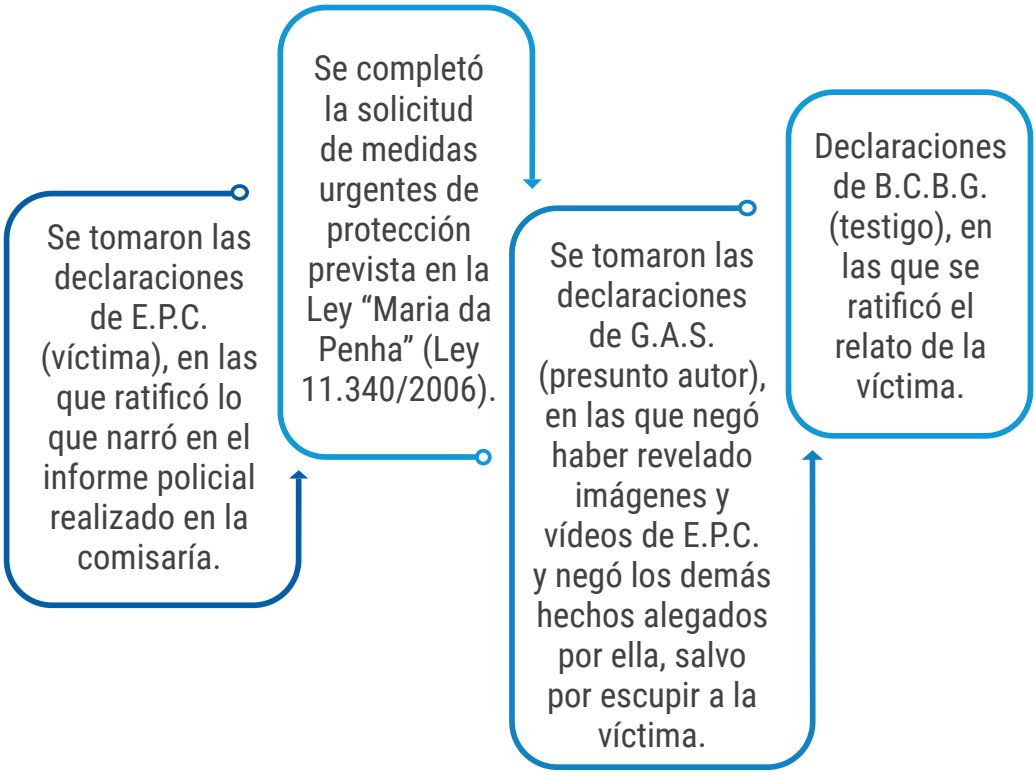


Figura 18: Proceso de investigación de seguimiento. **Fuente:** labSEAD-UFSC (2020).

Posteriormente, con el informe preliminar de la investigación de los agentes de policía y con los motivos enumerados anteriormente, el delegado de la policía emitió una carta al operador celular responsable de la terminal telefónica (61) 9XXXX-YYYY. Sin embargo, el operador de telefonía móvil informó de que no había datos de registro asociados a esta terminal.

Cabe señalar que dicha terminal estaba habilitada el 29/12/2018 y hasta mediados de enero, cuando el delegado se comunicó con el operador telefónico, no había datos de registro asociados a la misma. En este sentido, cabe señalar que, en el modelo del sistema telefónico brasileño, el registro de usuarios de teléfonos móviles prepagados se realiza mediante autodeclaración del usuario, de acuerdo con la Ley 10.703/2003.

Saber más

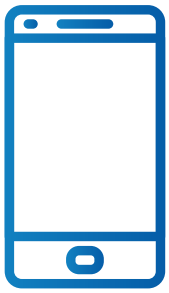
La Ley 10.703/2003 establece que el usuario que deje de cumplir con el registro de su dispositivo telefónico estará sujeto a una multa de hasta $50,00 (cincuenta reales) por infracción.

Puedes acceder a la ley al hacer clic en el *link*: http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.703.htm

También puedes mejorar tus estudios conociendo en su totalidad la Ley Maria da Penha, al hacer clic en el *link*: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm

Aunque existe tal dispositivo legal, es común que los delincuentes compren chips de telefonía prepago y no realicen su registro o incluyan datos falsos. De tal forma, con respecto a la ausencia de registro, el operador telefónico informó que el chip de la terminal telefónica (61) 9XXXX-YYYY se insertó en el aparato telefónico con IMEI 3532XXXXXXXXXXX.

En las fuentes abiertas, es posible verificar que dicho IMEI es de un aparato de telefonía celular modelo XXXX del fabricante YYYY.



En fuentes abiertas, es posible verificar que dicho IMEI es de un modelo de teléfono móvil RAZR D1 del fabricante Motorola. Dicho aparato presenta un valor de mercado alrededor de R$ 500.00.

Figura 19: Modelo de dispositivo celular utilizado por el autor de delitos cometidos contra E.P.C. **Fuente:** labSEAD-UFSC (2020).

El objetivo de la investigación empleó un chip prepago para cometer el crimen, que fue habilitado el 29/12/2018, es decir, tres días antes del crimen, lo que nos hace suponer que este es un chip que fue usado única y exclusivamente para el delito

y luego fue descartado. Si tenemos en cuenta esto, es poco probable que el objetivo haya utilizado el modelo de dispositivo XXX del fabricante YYY también de una manera desechable, ya que aunque no se encuentra entre los aparatos más caros en el mercado, es poco probable que haya desecho dicho dispositivo frente a la pérdida inminente de R$ 500.

Al tener en cuenta esta hipótesis, el delegado de la policía emitió otra carta al operador de telefonía móvil, esta vez, en orden cronológico, de todos los chips insertados en el dispositivo IMEI 3532XXXXXXXXXXX. En respuesta, el operador informó que se utilizaron tres terminales telefónicas en el dispositivo IMEI 3532XXXXXXXXXXX, ya que todas ellas estaban registradas en nombre de G.A.S.

> Es decir, aunque G.A.S. utilizó un *chip* de celular anónimo prepago (es decir, sin datos de registro) para divulgar sin consentimiento videos y fotos íntimas de E.P.C., fueron insertados en el mismo teléfono celular utilizado por el crimen, tres chips que fueron registrados a su nombre.

Cabe señalar que, en este caso, no fue necesario que el delegado policial solicitara al Poder Judicial la eliminación del sigilo de los datos telemáticos de la cuenta de WhatsApp involucrada, ya que la autoría fue dilucidada antes de que fueran necesarias las medidas cautelares, con el simple envío de oficios que solicitaran los datos a los operadores telefónicos. Sin embargo, si no se hubiera aclarado la autoría, el delegado de la policía tendría que solicitar al Poder Judicial eliminar el sigilo de los datos telemáticos de la cuenta de WhatsApp involucrada, y la empresa WhatsApp informaría al delegado los datos que permitirían individualizar y llegar al autor.

Con esto, los elementos de investigación nos permitieron concluir, más allá de una duda razonable, la existencia de la importancia del delito de revelación de una escena de violación o de una escena de violación de vulnerables (según lo dispuesto en el párrafo 1 del art. 218-C del Código Penal).

De hecho, las declaraciones de E.P.C. (comunicación) (fls. 8 y 9), las declaraciones de B.C.B.G. (testigo) (fl. 34) y las declaraciones de B.C.B.G. (testigo) (fl. 35) materializan el delito de revelación de la escena de violación o escena de violación de situaciones vulnerables, sexuales o pornografía practicadas en contra de E.P.C. desde la terminal telefónica (61) 9XXXX-AAAA, mientras recae en G.A.S la autoría de estos crímenes.

Además, la investigación permitió concluir, más allá de una duda razonable, la existencia de la importancia del delito de falsedad ideológica (según lo previsto en el art. 299 del CP), porque G.A.S., con el fin de cambiar la verdad sobre el hecho legalmente relevante, omitió, en un documento privado, los datos catastrales relativos al uso de la terminal telefónica (61) 9XXXX-AAAAA, datos que debe proporcionar de conformidad con el artículo 4 de la Ley 10.703/2003.

En cuanto a los demás hechos, la investigación realizada por la Policía Civil del Distrito Federal permitió la construcción de una prueba mínima *standard* que nos permite concluir, por encima de una duda razonable, la existencia de la importancia del delito de perjuicio real (párrafo 2 del art. 140 del CP) practicado por G.A.S. Por tal motivo, si aplicamos el análisis técnico-jurídico de los hechos y elementos de información reunidos en la investigación policial, el delegado de policía acusó a G.A.S. de la comisión de algunos delitos, que se pueden identificar en la siguiente imagen.

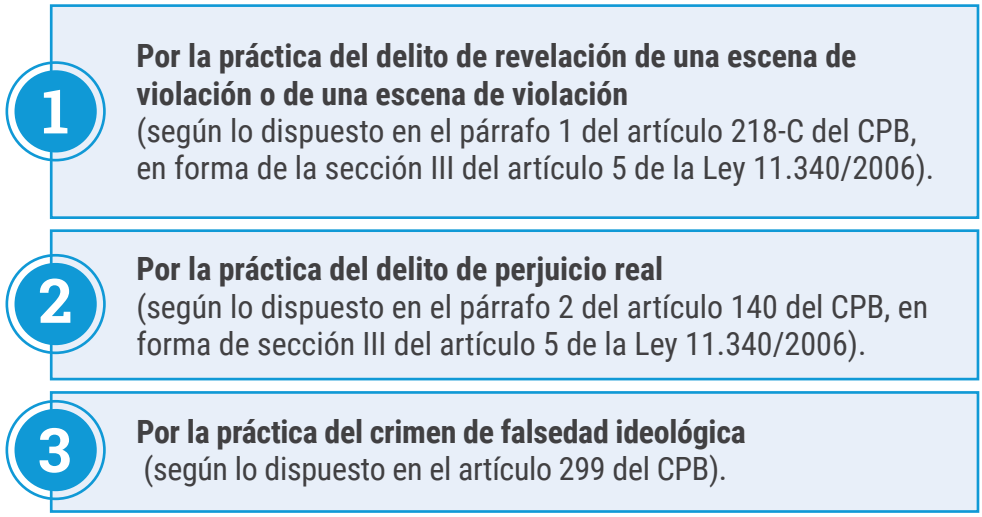


Figura 20: Crímenes que indicaron el autor del delito. **Fuente:** labSEAD-UFSC (2020).

Por lo tanto, hemos concluido nuestra clase sobre lecciones prácticas en el proceso de investigación de delitos electrónicos.

Ahora, procederemos a nuestra clase que abordará la estructura de los documentos utilizados en la investigación de estos crímenes.

Clase 2 – Estructura de los Documentos Utilizados en la Investigación de Delitos Cibernéticos

CONTEXTUALIZANDO...

El objetivo de esta parte del curso es presentar, a través de un enfoque práctico, la estructura de los principales documentos que el investigador cibernético necesita conocer, para poder aplicarlos en su rutina operativa. Por lo tanto, continuaremos con nuestros estudios y analizaremos la estructura de los documentos oficiales utilizados en el proceso de investigación de crímenes digitales.

RESUMEN HISTÓRICO

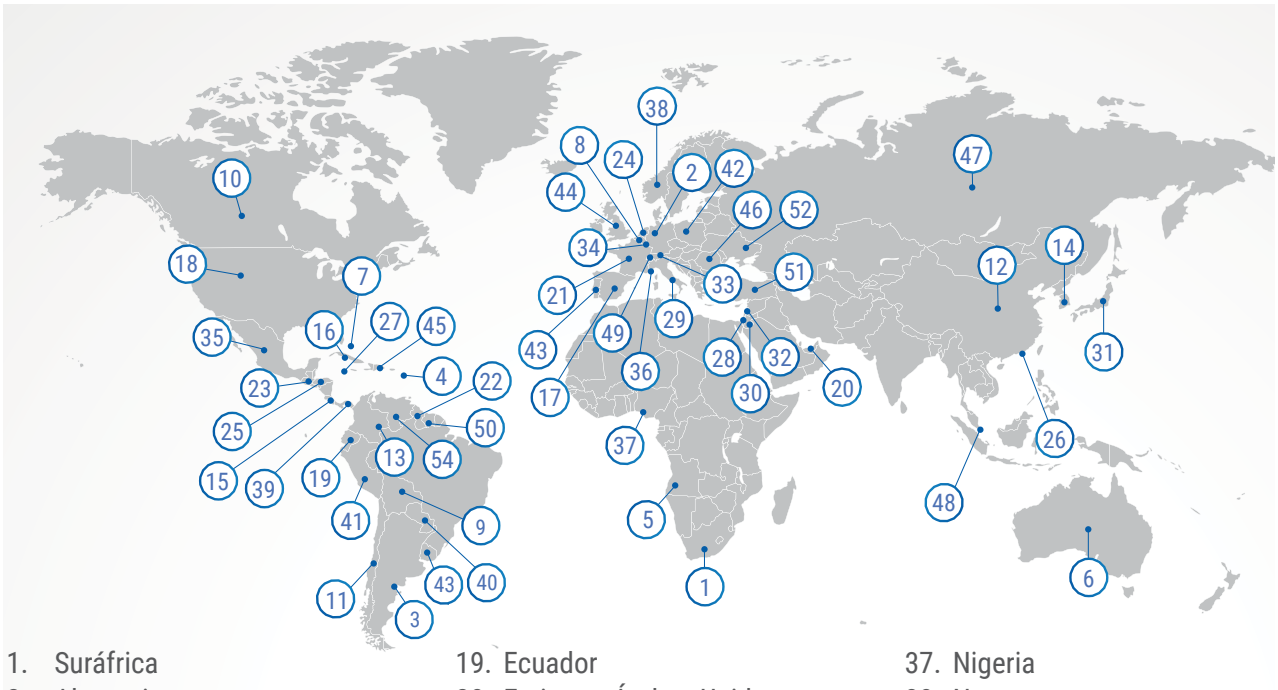
No es contradictorio traer al contexto actual, característicamente virtualizado, la producción textual y la importancia de la creación de documentos. Incluso cuando se trata de autorizaciones en un entorno cibernético y la prestación de servicios exclusivamente digitales, el trabajo de generación de solicitudes administrativas y judiciales sigue siendo indispensable, en la mayoría de los casos. Esta es una realidad global, y no es exclusiva de las investigaciones llevadas a cabo por organismos nacionales.

En primer lugar, debe tenerse en cuenta que rara vez hay un caso en el que participen únicamente proveedores brasileños. Los delitos se cometen habitualmente en los entornos virtualizados de aplicaciones y sitios *web*, especialmente en redes sociales y de mensajería, que conforman este universo. Estas soluciones tecnológicas, ampliamente utilizadas por todas las naciones del mundo, incluidos los brasileños, son generalmente desarrolladas y mantenidas por empresas estadounidenses y europeas. Algunas aplicaciones chinas también son utilizadas, pero no son la mayoría.

Tanto en los Estados Unidos como en la Unión Europea existe un sistema jurídico destinado a proteger la privacidad y los datos personales. Además, como hemos visto antes, existe una

convención internacional y multilateral sobre la cooperación entre países en la lucha contra la delincuencia virtual, la Convención de Budapest, de la que Brasil no es signatario. Por lo tanto, el país no está contemplado en las medidas de cooperación descritas en este importante pacto entre otros países.

Sin embargo, Brasil ha firmado tratados de cooperación mutua con algunos países en materia penal. En la actualidad, son los países que se presentan la siguiente imagen:



1. Suráfrica
2. Alemania
3. Argentina
4. Antigua y Barbuda
5. Angola
6. Australia
7. Bahamas
8. Bélgica
9. Bolivia
10. Canadá
11. Chile
12. China
13. Colombia
14. Corea del Sur
15. Costa Rica
16. Cuba
17. España
18. Estados Unidos de América
19. Ecuador
20. Emiratos Árabes Unidos
21. Francia
22. Guyana
23. Guatemala
24. Holanda
25. Honduras
26. Hong Kong
27. Islas Caimán
28. Israel
29. Italia
30. Jordania
31. Japón
32. Líbano
33. Liechtenstein
34. Luxemburgo
35. México
36. Mónaco
37. Nigeria
38. Noruega
39. Panamá
40. Paraguay
41. Perú
42. Polonia
43. Portugal
44. Reino Unido (Gran Bretaña)
45. República Dominicana
46. Rumania
47. Rusia
48. Singapur
49. Suiza
50. Surinam
51. Turquía
52. Ucrania
53. Uruguay
54. Venezuela

Figura 21: Países con Tratado de Cooperación Mutua con Brasil.
Fuente: labSEAD-UFSC (2020).

En el *site* del Ministerio de Justicia (www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/orientacoes-por-pais), es posible extraer información sobre el procedimiento de solicitud aplicable a cada país en materia penal. Una vez revisado, podemos llegar a la conclusión de que, en todos los casos, las solicitudes son formales.

Brasil, por ejemplo, ha establecido con los Estados Unidos de América la Asistencia Jurídica Mutua de Riaty (MLAT) — Acuerdo de Asistencia Jurídica en Materia Penal — recibido en la ley brasileña por el **Decreto Nº 3 810, de 2 de mayo de 2001.** Este instrumento internacional presenta procedimientos específicos para las solicitudes de datos telemáticos.

En el país donde se concentran la mayoría de los servicios *web* y aplicaciones utilizadas en Brasil, depende de usted, investigador, conocer la norma. La mejor manera de encontrarla puede ser la cooperación internacional para obtener pruebas.

Saber más

Para conocer la redacción completa del Decreto 3.810/2001, haz clic en *link*: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm

En resumen, el objetivo de este curso no es el tema de "Cooperación Jurídica Internacional para Investigaciones Cibernéticas", pero lo que se pretende demostrar es que la obtención de información sigue condicionada a la formalización de las solicitudes. La labor jurídica en este contexto sigue siendo importante.

El uso de procedimientos de "*hacking* ético" para llevar los vestigios electrónicos a la recopilación de pruebas sigue siendo la base de un amplio debate doctrinal, rara vez autorizado por los tribunales judiciales. Por lo tanto, se exalta la importancia del conocimiento sobre la estructura de un documento de solicitud,

que debe tener el **investigador cibernético**, ya sea que esté una función operativa, o quien presida un procedimiento, como es el caso de la autoridad policía.

Por lo tanto, demostraremos el método de solicitar la preservación de datos a través de oficios.

PEDIDOS DE PRESERVACIÓN DE DADOS POR MEDIO DE OFICIOS

La solicitud de conservación de datos se puede realizar directamente en plataformas digitales desarrolladas por los propios proveedores, como Facebook, Instagram y WhatsApp. Sin embargo, en algunos casos, como el de Google Inc., se requiere que una comunicación oficial, firmada por la autoridad requirente, sea enviada a través de su plataforma.

En otros casos, al igual que con Apple, que aún no tiene una plataforma de Law Enforcement (aplicación de la ley), se exige que este documento sea enviado como anexo a un pedido oficial vía *email*.

> El oficio puede entenderse como una comunicación escrita, formal y ceremoniosa, utilizada en el servicio público, intercambiada entre autoridades que desempeñan las mismas funciones o emitida por funcionarios con cargos inferiores a sus superiores jerárquicos, con el fin de presentar una solicitud o reclamación oficial.

En Brasil, este tipo de documentos también se ha utilizado comúnmente como instrumento formal para el diálogo entre la autoridad brasileña y los receptores extranjeros, especialmente directores y/o presidente de personas jurídicas. En este contexto, se refiere a las empresas que proveen servicios de *internet*, internacionalmente denominadas ISP (Internet Service Provider).

Bajo los términos del Marco Civil de Internet (Ley 12.965/2014), existe un proveedor de aplicaciones y un proveedor de conexión.

Estas organizaciones desempeñan un papel importante en la composición de la red Internet, ya que son puntos de esta red de información entrelazada. Pueden ser responsables del tráfico de paquetes de datos, alojar contenido, proporcionar un servicio de correo electrónico o servir como medio de comunicación entre personas en tiempo real. Estos son apenas algunos de los servicios dentro de cientos de otros que realizan empresas de todo el mundo.

Figura 22: Empresas de prestación de servicios de *internet*. **Fuente:** labSEAD-UFSC (2020).

Todo el flujo que pasa, de alguna manera, a través de la infraestructura de estas empresas y que puede, en teoría, ser almacenado, incluso si cuenta con encriptación que impida el acceso a sus contenidos.

> En el espacio virtual, estos datos se estructuran, para así transformar dígitos binarios en entornos gráficos fáciles de usar, capaces de recibir y enviar las manifestaciones de sus usuarios en milisegundos, quienes ignoran estos procesos algorítmicos complejos.

Para el investigador, esta cadena de eventos, creada en *bits* o en un lenguaje superior capaz de revelar el desempeño de protocolos en el entorno computacional investigado, constituye la materia prima de su trabajo. Debido a la característica extremadamente dinámica de los delitos cibernéticos, sus vestigios son rápidamente borrados o sobrescritos de los bancos en los que se han depositado pruebas de delitos, los cuales se consideran altamente perecederos. **De ahí la importancia de su preservación.**

Figura 23: La importancia de la preservación de datos para la prueba de delitos cibernéticos.
Fuente: Pixabay (2020).

En este sentido, después de la contextualización sobre la naturaleza del instrumento de comunicación y el tipo de empresas receptoras y objeto de preservación, conoceremos la estructura del documento que solicita la preservación de datos.

El documento

Para este tipo de documentos, cuya naturaleza está exclusivamente protegida, no se recomienda el uso de textos muy técnicos o detallados, teniendo en cuenta que esto puede representar motivo de retraso en la preparación y envío del documento. Otro riesgo a tener en cuenta es que la empresa entiende que sólo debe conservar parte de los datos que poseen, a partir de la interpretación de la solicitud.

Por esta razón, es preferible que el texto exprese la pretensión de que el proveedor conserve durante el período legal (Ley 12.965/2014) todos los datos de la cuenta del usuario (cuenta de *email*, perfil de red social, página alojada, entre otros).

> La solicitud, en este formato genérico, no viola en modo alguno los derechos de privacidad o cualquier otro garantizado en las disposiciones legales, ya que no se trata del acceso a los datos, sino sólo una solicitud de salvaguardia de estos activos informativos para la futura aplicación del derecho penal y procesal penal.

En cuanto a la forma de mención a los destinatarios, el escritor del oficio debe utilizar la técnica editorial regulada en su Unidad de Federación o corporación. Por lo tanto, los elementos textuales, como los pronombres de tratamiento, saludos y el lugar donde deben introducirse los datos del proveedor, necesitan cumplir estos parámetros.

En este material no se presentará una lista de proveedores por varias razones, entre las cuales se encuentran, el riesgo de que la información se desactualice. Sin embargo, te recomendamos buscar esa información en fuentes abiertas de la red *internet*. Resaltaremos algunos consejos en la siguiente imagen.

1

Proveedores brasileños

El nombre del proveedor se utiliza como palabra clave en los motores de búsqueda, seguido de las palabras “empresa” y “CNPJ”. Como resultado, aparecerán diversos sitios *web* especializados en la presentación de información de registro de la empresa, los cuales aportarán varios datos sobre el proveedor, incluyendo la dirección, *email* y número de teléfono del departamento legal. Estos canales de contacto son muy importantes porque, a través de ellos, la agencia solicitante debe hacer contacto previo e informarse sobre el mejor medio para enviar la comunicación.

2

Proveedores internacionales

En el caso de empresas como Facebook, Instagram y WhatsApp, no es necesario enviar oficios escaneados para la solicitud de conservación.

Simplemente rellena los campos requeridos del sitio *web*. En el caso de la empresa Google Inc., el profesional de la aplicación de la ley y perteneciente al organismo gubernamental debe registrarse en la plataforma LERS (https://lers.google.com/signup_v2/landing) para subir el archivo escaneado. Los otros sitios *web* suelen recibir oficios vía *email*. Cabe destacar que, en cualquier caso, se debe determinar si la empresa extranjera tiene representante legal en Brasil, ya que la dirección que se ingresará en la oficina será la de este país. Para conocer esta representación, se recomienda emplear el consejo que se muestra para los proveedores nacionales.

Figura 24: Solicitud para proveedores nacionales e internacionales. **Fuente:** labSEAD-UFSC (2020).

Adicionalmente, sobre lo que respecta a los proveedores internacionales, en caso de que no se logre identificar ningún representante en suelo brasileño, se sugiere ubicar los datos del proveedor extranjero, en el siguiente *link*: www.search.org/resources/isp-list, o buscar en la página oficial de la empresa, en los términos y las políticas de uso de los servicios.

SOLICITUDES DE DATOS DE REGISTRO DE USUARIOS DE SERVICIOS PRESTADOS POR PROVEEDORES DE APLICACIONES

La Ley 12.965/2014, el Marco Civil del Internet, en su quinto artículo, define las aplicaciones de *internet* como "el conjunto de funcionalidades a las que se puede acceder a través de un terminal conectado a internet". Por lo tanto, los proveedores de aplicaciones son las empresas que desarrollan y gestionan estas "funcionalidades virtuales".

La solicitud de datos de registro de los usuarios de los servicios de aplicación tiene como base jurídica el tercer párrafo del artículo 10 de dicha ley. Esta disposición legal también confiere la prerrogativa de que las autoridades administrativas puedan solicitar dicha información sin necesidad de autorización judicial. Este dispositivo legal debe expresarse en el documento, justificando la facultad de solicitar datos por parte del postulante.

> *Art. 10 - El mantenimiento y disponibilidad de los registros de conexión y acceso a las aplicaciones de internet que trata esta Ley, así como los datos personales y el contenido de las comunicaciones privadas, deben servir a la preservación de la intimidad, privacidad, honor e imagen de las partes involucradas directa o indirectamente.*
>
> *§ 3º Las disposiciones del caput no impiden el acceso a los datos de registro que proporcionen calificación personal, membresía y domicilio, en la forma de la ley, por las autoridades administrativas que tengan competencia legal para su solicitud. (BRASIL, 2014, traducción nuestra).*

Cabe destacar que el Marco Civil del Internet fue regulado por el Decreto 8771/2016, que obliga a las autoridades administrativas, a las que se refiere el artículo mencionado, a indicar, además de la base jurídica de la competencia expresa para el acceso, la motivación para solicitar acceso a los datos catastrales.

Por este motivo, algunas empresas proveedoras multinacionales, Como Google, Facebook, Instagram y WhatsApp exigen que el solicitante demuestre que el crimen investigado sea objeto de la Ley de Organización Criminal o de la Ley de Lavado de Dinero o, inclusive, de la Ley de Terrorismo.

Otros delitos, como el artículo 122 del Código Penal: La "inducción, instigación o ayuda al suicidio" ha sido aceptada por el departamento jurídico de los proveedores de solicitudes como justificadores del suministro de datos catastrales sin una orden judicial. Esta interpretación se flexibilizó debido al fenómeno que ocurrió en 2017 en Brasil y en el mundo, en el que los delincuentes invitaron a niños y adolescentes a desafíos virtuales con graves consecuencias, incluyendo autolesiones y suicidio. En muchos estados brasileños se han observado casos de desafíos conocidos como la "Ballena Azul".

Saber más

El desafío de la "ballena azul" contribuyó al crecimiento de la discusión sobre el suicidio juvenil. Lee más sobre este desafío que ha traído graves consecuencias.

Lee el artículo al hacer clic en el *link*: https://brasil.elpais.com/brasil/2017/04/27/politica/1493305523_711865.html

El decreto 8771/2016 define como **datos catastrales** sólo los referidos a la pertenencia, dirección y cualificación personal, que son entendidos como nombre, apellido, estado civil y profesión del usuario. En los aspectos relacionados con el **destinatario del pedido**, se deben seguir las mismas pautas presentadas en el ítem anterior, con respecto a la solicitud de preservación de datos. En cuanto al **objeto de la solicitud**, parece evidente que son los datos de registro del usuario de la cuenta investigada (cuenta de *email*, perfil, página alojada, entre otros).

Sin embargo, existe una valiosa reflexión sobre el tema, que trata de la postulación judicial de los datos. En este sentido, se señala a la atención del agente de la ley, que a veces puede ser un abogado, la importancia de saber cuál es el objeto de su solicitud.

Por lo tanto, es válido el razonamiento sobre la actividad profesional ejercida por el destinatario del proceso. Después de todo, este último sólo puede cumplir aquellas reclamaciones que se dirijan a los datos que posee. Un ejemplo de esto sería una organización que se especializa en servicios de mensajería que no puede cumplir con el objeto de un oficio que le pide los datos de una bandeja de correo electrónico. **En este aspecto radica el mayor número de errores que justifican la devolución de solicitudes con una respuesta negativa.**

En muchos casos, la autoridad hace uso de las sanciones descritas en el artículo 12 de la Ley Marco Civil del Internet, con el fin de sancionar a las empresas que no le han entregado datos. La mayoría de estos litigios terminan en los tribunales, e incluso si el magistrado confirma la obligación legal de la empresa, ésta no puede proporcionar la información simplemente porque no la posee.

Vale la pena recordar que el Decreto 8.771/2016, regulador del Marco Civil del Internet, en su artículo once, señala que "el proveedor que no recopile datos catastrales deberá informarle a la autoridad solicitante de este hecho, sin la obligación de proporcionar esos datos".

Sin embargo, es necesario comprender el modelo de negocio de la empresa, qué datos opera y qué información sobre sus clientes necesita para funcionar. Veamos un ejemplo de un portal de noticias que almacena el contenido de sus usuarios en su repositorio virtual para su publicación.

Este portal requiere que los escritores sólo hagan un pequeño registro en su plataforma, rellenando un formulario sencillo cuyos campos son: nombre, seudónimo (opcional), *email* y contraseña. De los cuatro datos, solo la dirección de correo electrónico y la contraseña de acceso son validables, es decir, deben ser verdaderos, ya que la primera es la clave principal para *login* en el *site*, seguido de la contraseña de acceso. Los otros son sólo textos, que pueden ser falsos o modificados en cualquier momento. El sitio *web* se puede programar para recopilar la dirección IP del usuario cada sesión.

En el contexto del ejemplo anterior, es fácil ver que, para el funcionamiento de la plataforma, no es esencial que el proveedor que tiene el número de terminal telefónico de los

autores desarrolle su proceso operativo. Tampoco le interesa el número de identificación o la dirección física donde residen. **A la organización sólo le importa que sus clientes registren sus credenciales de acceso, que sólo puede ser una dirección de *email* y una contraseña.**

Por otro lado, el contenido de los textos es su principal activo informativo, es decir, lo que le agregará valor. Una vez que se le pida que localice un texto por una palabra clave, sin duda debe disponer de los medios para satisfacer la solicitud, teniendo en cuenta los plazos legales que requieren almacenar datos. Esta es la información que se supone que está en posesión de la empresa.

Otros ejemplos interesantes para ilustrar esta relación entre un modelo de negocio de empresa *versus* los activos de información almacenados son los de las empresas Google y Apple.

Cuando se trata de puntos convergentes, ambas empresas ofrecen servicios de almacenamiento de datos en la nube a sus usuarios y son responsables de desarrollar los dos sistemas operativos móviles más utilizados en el planeta: Android e IOS. También disponen de todo aquello que los *smartphones* registran o navegan en términos de datos, es decir, que sean objeto de *backup* en sus nubes de almacenamiento (fotos, videos, datos de aplicaciones, entre otros). Las dos empresas también desarrollan navegadores *web* y recopilan datos de *desktops*, además de ofrecer servicios de correo electrónico. En estas áreas, Google lidera el mercado porque Gmail y Google Chrome son incomparablemente más utilizados que los productos de Apple. Por el contrario, Apple tiene un sistema operativo para *desktops* y Google no.

En Brasil, solo Apple posee tiendas físicas y vende dispositivos fabricados por ella misma, así como puede acreditar oficialmente a terceros para realizar reparaciones (Apple RetailStores). También funciona con pedidos, al entregar

dispositivos comprados en tiendas virtuales. A diferencia de los Estados Unidos, donde Google también tiene ventas en tiendas y vende sus dispositivos Google Pixels.

Al tener en cuenta esta información general sobre las dos empresas y los parámetros legales establecidos en la Ley 12.965/2014, el investigador puede formular algunas conclusiones, que pueden ser observadas en la siguiente imagen.

Figura 25: Conclusiones hipotéticas sobre el análisis de las empresas de Apple y Google. **Fuente:** labSEAD-UFSC (2020).

En la hipótesis que hemos visto en la imagen anterior, vale la pena mencionar que Apple tiene mejores posibilidades de atender una solicitud de datos de registro, ya que ofrece servicios que operan en el mundo natural, es decir, tiendas físicas y entregas a domicilio de dispositivos comprados en sus tiendas virtuales. Debido a estas actividades, podemos destacar algunos puntos, que podemos observar en la siguiente imagen.

Figura 26: Información del usuario que es posible solicitarle a la empresa Apple. **Fuente:** labSEAD-UFSC (2020).

Por último, cuando se trata de la ubicación de la persona, los usuarios de la empresa Google son definidos más fácilmente. Esta empresa es la que mantiene el mayor beneficio de la monetización de los datos de sus clientes, incluidos los operadores del sistema operativo Android.

> Los datos relacionados con la posición de una persona y en un determinado espacio de tiempo son considerados de alto valor para la empresa, ya que estas coordenadas son comercializadas en subastas virtuales y adquiridas por empresas de *ecommerce* y publicidad.

La lógica es fácil de entender: si una empresa tecnológica que se ocupa de hostelería, turismo o entrega de alimentos tiene conocimiento sobre la ubicación de un usuario, esto aportará una gran ventaja competitiva porque ofrecerá algo muy específico e interesante para el consumidor. Por ejemplo: un paquete turístico, que incluye paseos y visitas.

Otro tipo de entidad jurídica que contiene datos de ubicación son las que se especializan en la transacción de servicios de movilidad, las llamadas “aplicaciones de viaje pagado”. En Brasil, los ejemplos son: UBER, Cabify y 99POP. Estas empresas almacenan, además de los datos de registro y financieros de sus clientes, información sobre los viajes realizados. Las empresas que prestan el mismo servicio, pero

en el sector de la hostelería, también pueden informar si una persona se ha alojado en un punto geográfico determinado.

REPRESENTACIONES DE MEDIDAS CAUTELARES EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS

En cuanto a la utilidad de solicitar datos para la investigación cibernética a través del envío de oficios, no es posible obtener de esta manera toda la información necesaria y útil para la investigación cibernética.

Como vimos anteriormente, el Marco Civil del Internet, por un lado, **permite la solicitud de datos sin una orden judicial** por las autoridades del Ministerio Público, Policía Civil y Policía Federal. Por otro lado, el Marco Civil del Internet establece que las autoridades del Ministerio Público, la Policía Civil y la Policía Federal **sólo pueden tener acceso a registros de conexión (o acceso), datos personales y contenidos de comunicaciones mediante orden judicial.**

En este contexto, las representaciones de medidas cautelares se incluyen en el ámbito de la investigación de delitos cibernéticos, que son el instrumento utilizado por el delegado policial para solicitar una orden judicial al Poder Judicial, dirigida a empresas de aplicaciones de *internet* o proveedores de conexión, para que estas empresas proporcionen registros de conexión (o acceso), datos personales y contenido de comunicaciones.

> Recordemos que Brasil ha adoptado, por regla general, que las pruebas relacionadas con la práctica de los delitos se presenten en un contradictorio judicial, por lo que el juez no puede justificar su decisión exclusivamente sobre la información recogida en la investigación, es decir, **el juez no puede dictar su condena exclusivamente con elementos derivados de la investigación policial.**

A pesar de esto, conforme fue explicado, el artículo 155 del Código Procesal Penal (CPP) permite, de manera extraordinaria, que la prueba producida en la fase de investigación sea utilizada como elemento principal de la condena del juez: **se trata de las pruebas cautelares, las cuales no están sujetas a repetición y son producidas con antelación.** Así mismo, en la investigación de delitos cibernéticos, registros de conexión (o acceso), los datos personales y el contenido de las comunicaciones privadas son evidencias caracterizadas por la necesidad y urgencia (evidencia cautelar) y se obtienen a través de la representación del delegado de la policía al Poder Judicial.

Por lo tanto, es parte integrante de la investigación de seguimiento la representación ante el Poder Judicial mediante la eliminación del sigilo telemático de los objetivos de la investigación, así como parte integrante de esta fase de investigación la presentación ante el Poder Judicial para la eliminación del sigilo de las comunicaciones telemáticas. Paralelamente, también existe, aunque en un momento posterior, la presentación ante el Poder Judicial para el registro e incautación domiciliaria.

La presentación judicial para la eliminación del sigilo telemático se rige por el Marco Civil del Internet y consta de tres partes, que destacamos en la siguiente imagen.

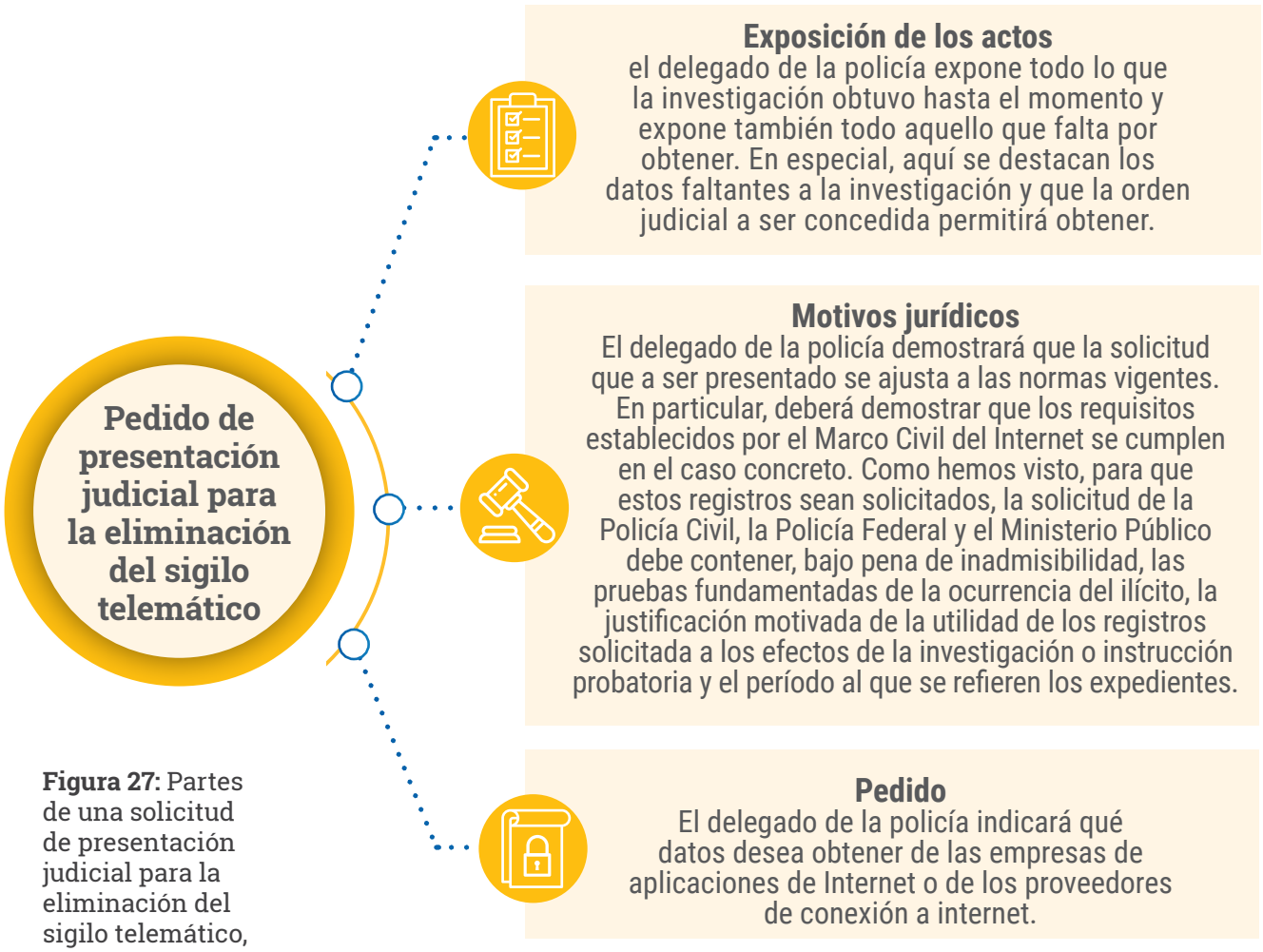


Figura 27: Partes de una solicitud de presentación judicial para la eliminación del sigilo telemático, de acuerdo con el Marco Civil del Internet. **Fuente:** labSEAD-UFSC (2020).

La presentación judicial para la búsqueda e incautación domiciliaria, por otro lado, no está regida por el Marco Civil del Internet, pero sí por el Código Procesal Penal (CPP), y también está compuesta de tres partes, las cuales podremos identificar en la siguiente imagen.

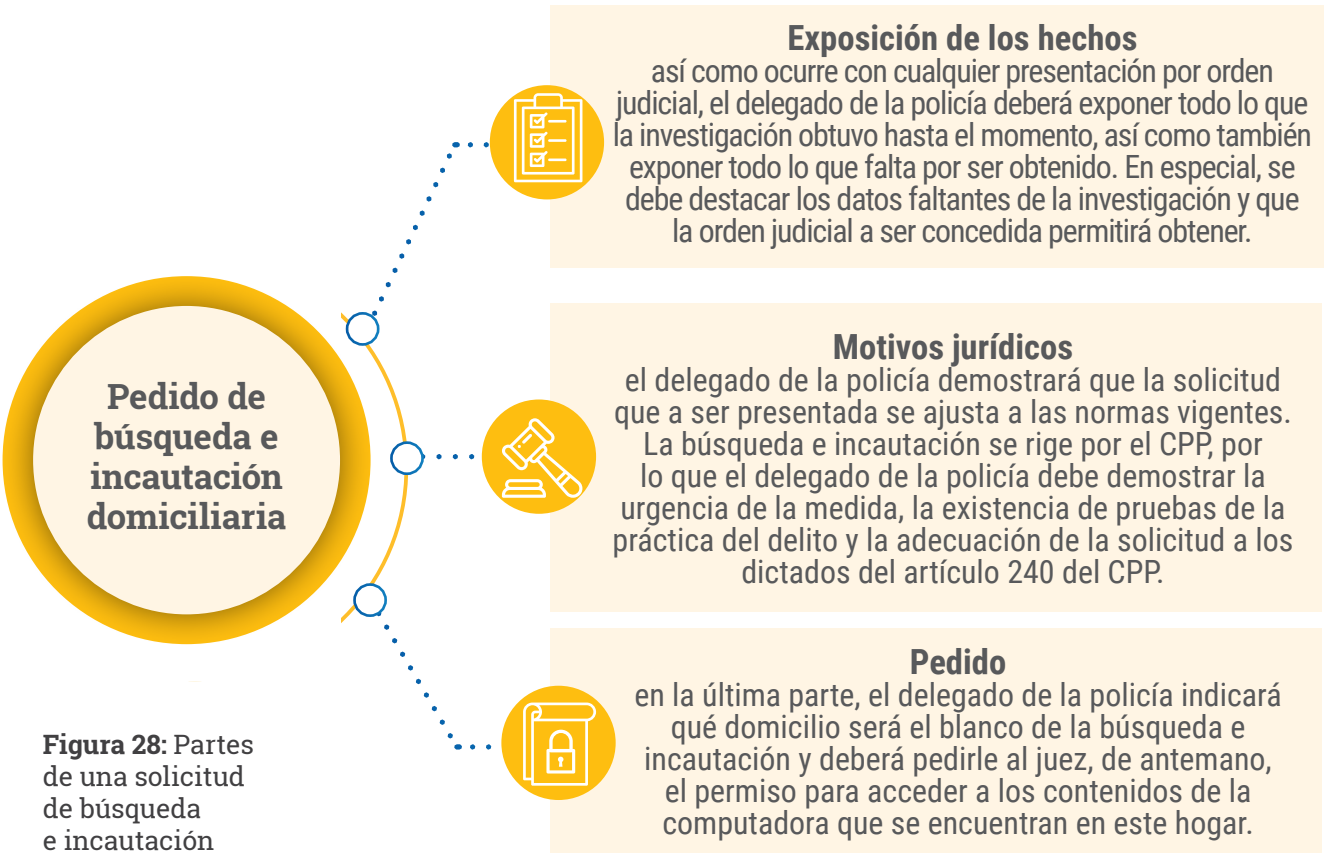


Figura 28: Partes de una solicitud de búsqueda e incautación domiciliario, de conformidad con el Código de Procedimiento Penal. **Fuente:** labSEAD-UFSC (2020).

En vista de esto, continuaremos nuestros estudios y conoceremos las solicitudes de datos de registro de usuarios de servicios prestados por proveedores de conexión.

SOLICITUDES DE DATOS DE REGISTRO DE USUARIOS DE SERVICIOS PRESTADOS POR PROVEEDORES DE CONEXIÓN

Este tipo de solicitud, en la mayoría de los casos, se produce después de las solicitudes de eliminación del sigilo de los datos telemáticos, contenidas en las medidas cautelares presentadas. Esto se debe a que el flujo de investigación cibernética comienza con solicitudes a los proveedores de aplicaciones, ya que en el entorno de los servicios que prestan es que se realizan los actos ejecutorios.

> En otras palabras, los delitos ocurren en sistemas desarrollados y gestionados por proveedores de aplicaciones, que ofrecen los siguientes servicios: comunicación por *email*, aplicaciones de mensajería, *ecomerce*, redes sociales, portales de noticias, entre otros.

Para fines de fijación y aprendizaje, seguiremos el flujo, considerado como "más común". Es importante considerar las siguientes abreviaciones: "UP" para la Unidad de Policía, "PA" para el Proveedor de Aplicaciones y "PC" para el Proveedor de Conexión. Ten en cuenta la siguiente imagen de un delito ocurrido en un entorno de aplicación (*email*, aplicación de mensajería, entre otros).

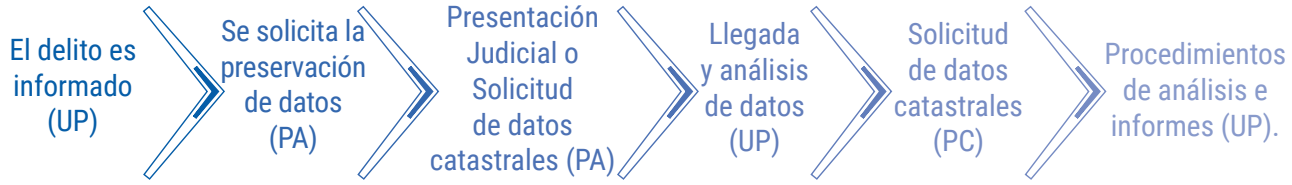


Figura 29: Ejemplo de delito ocurrido en un entorno de aplicación.
Fuente: labSEAD-UFSC (2020).

Ten en cuenta otro ejemplo en la siguiente imagen. Pero ahora, de un crimen que ocurrió en un ambiente de *sites* (*ecommerce, blogs*, entre otros).

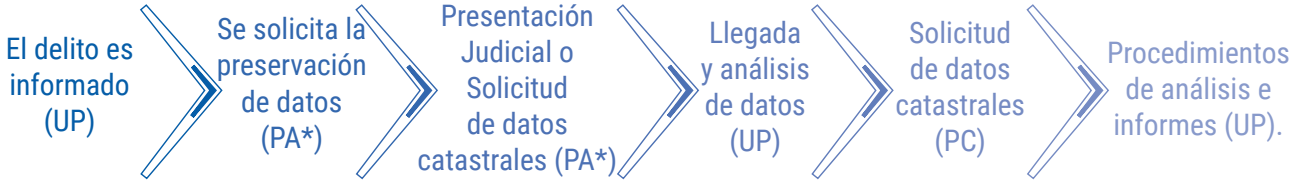


Figura 30: Ejemplo de crimen ocurrido en un ambiente de *sites*.
Fuente: labSEAD-UFSC (2020).

Al seguir el flujo de la investigación, la unidad de policía recibirá, además de los datos de registro de los propietarios de las cuentas investigadas, los registros de sus conexiones (IP/*login*).

Saber más

La conexión a *internet* es la habilitación de un terminal para enviar y recibir paquetes de datos a través de *internet*, a través de la asignación o autenticación de una dirección IP. El **registro de conexión** es el conjunto de informaciones referentes a la fecha y hora de inicio y finalización de una conexión a *internet*, su duración y la dirección IP utilizada por el terminal.

Vale la pena recordar que los delitos ocurren en el entorno de la aplicación, pero debe tenerse en cuenta que se trata de aplicaciones *web*, es decir, programas cuyo funcionamiento está condicionado al acceso de sus usuarios a la red de *internet*. De hecho, solo las empresas responsables de proporcionar la conexión (proveedores de conexión) almacenan información sobre la ubicación donde se originó un acceso desde un protocolo IP. Por esta razón, estas entidades jurídicas son los destinatarios de la carta para solicitar datos de registro de los usuarios de IP conectadas.

Para recapitular lo que se enseñó en el módulo anterior, estos eventos entregados por los proveedores de aplicaciones suelen aparecer como archivos en formato ".pdf", y que aportan algunos elementos, que destacamos en la siguiente imagen.

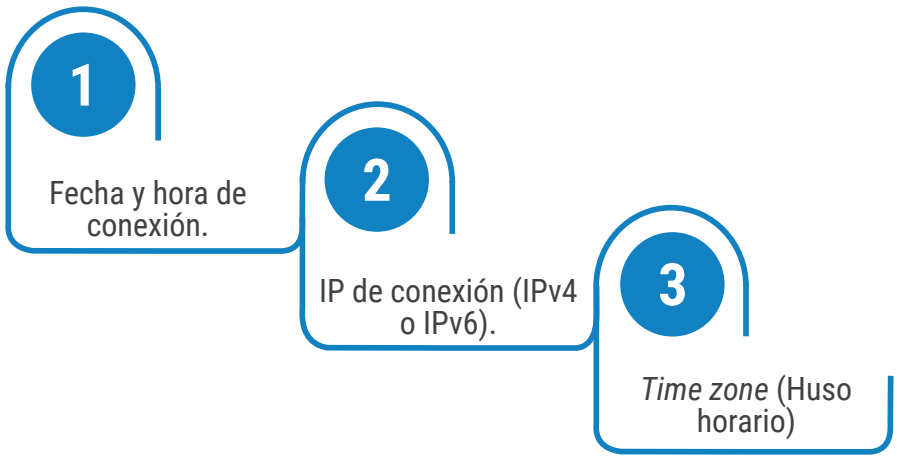


Figura 31: Elementos presentes en el archivo del proveedor de aplicaciones. **Fuente:** labSEAD-UFSC (2020).

Con relación al elemento "huso horario", presentado en la imagen anterior, vale la pena entender que este es cada una de las

veinticuatro áreas fusiformes en las que la Tierra está dividida convencionalmente, con el propósito de establecer el tiempo de acuerdo con el movimiento aparente del Sol. Este elemento también es una parte importante del "*login*" de conexión, el cual se refiere generalmente al huso horario de la región donde se encuentra el servidor en el que está almacenado los datos.

Sin embargo, si la aplicación fue accedida a través de una red proporcionada por un operador brasileño (proveedores de conexión: TIM, OI, Claro, Vivo, por ejemplo), es necesario realizar una **conversión de tiempo** para que estas empresas puedan proveer el nombre del usuario que inició sesión a través de esa IP en un día y hora determinados. La exactitud de la hora del evento es fundamental para identificar el origen de la conexión y la divulgación de la autoría criminal, ya que los IP se asignan dinámicamente en casi todos los casos resueltos.

A continuación se muestran las zonas horarias con la señalización de diferencias horarias con respecto al centro del mundo (UTC=0), que es la hora de Londres.

UTC	Universal Time Coordinated UTC =	0
CST	Central Standard Time	UTC+09:30
CDT	Central Daylight Time	UTC+10:30
CXT	Christmas Island Time	UTC+7
EST	Eastern Standard Time	UTC+10
EDT	Eastern Daylight Time	UTC+11
WST	Western Standard Time	UTC+8
WDT	Western Daylight Time	UTC+9
MDT	Mountain Daylight Time	UTC-6
PST	Pacific Standard Time	UTC-8
PDT	Pacific Daylight Time	UTC-7
NST	Newfoundland Standard Time	UTC-3,
NDT	Newfoundland Daylight Time	UTC-2
CET	Central European Time	UTC+1
CEST	Central European Summer Time	UTC+2
BST	British Summer Time	UTC+1

EET	Eastern European Time	UTC+2
EEST	Eastern European Summer Time	UTC+3
WET	Western European Time	UTC+0
WEST	Western European Summer Time	UTC+1

De acuerdo con las observaciones presentadas en los párrafos anteriores, se define la estructura del documento. Con respecto a la parte de la base jurídica y la mención al destinatario de la carta, se siguen las mismas instrucciones relativas a la solicitud de datos de registro de los proveedores de solicitudes.

La solicitud también tendrá el objetivo de "proporcionar los datos de registro", pero lo que se pretende son los datos del suscriptor de los servicios de red a los que se ha conectado el usuario de la aplicación. Por lo tanto, la solicitud debe estar redactada de la siguiente forma: "que proporcione los datos de registro del usuario de la IP (xxx), utilizado el día (xxx) y la hora (xxx) — (*time zone*)".

> La respuesta serán exactamente los datos de registro del suscriptor de la red a cuya IP se accedió. La empresa conserva esta información, ya que la mencionada IP pertenece a un bloque lógico que administra.

Vale la pena destacar que los proveedores de conexiones nacionales responden sólo a las solicitudes cuyos horarios **son convertidos a GMT-003.** Esto significa que Brasil utiliza el GMT (Greenwich Mean Time) por defecto, seguido de tres dígitos (positivos o negativos). Por tal motivo, no presenta gran reto el entender esta convención, si entendemos que GMT=UTC.

Así que si en Londres son las 10h00min UTC, también serían las 10h00min GMT 000. El mismo evento en Brasil sería a las 07h GMT -003, porque Brasil tiene -3 (menos tres) horas en comparación con Londres.

En la práctica, las empresas Google, Facebook, Instagram y WhatsApp siempre envían informes de *logs* en UTC. El investigador tendrá que restar tres (tres) horas de cada evento y escribirlo en el artículo seguido de la expresión "GMT-003".

Este proceso es aún más fácil gracias a la eliminación del horario de verano en el país. Cuando esto existía, o en caso de que vuelva a ser implementado, el analista deberá reducir sólo dos (2) horas en comparación con Londres.

Saber más

Hay páginas *web* que cuentan con herramientas que ayudan a realizar la conversión de horas. A continuación tenemos algunas recomendaciones.

www.timebie.com/timezone/universalbrasilia.php
www.worldtimebuddy.com/utc-to-gmt-converter

Finalmente, llegamos al final de un módulo más.

Aquí concluimos nuestros estudios que nos permitieron comprender más sobre:

- Crímenes cibernéticos en Brasil.
- Concepto de espacio virtual e *internet*.
- Conocimiento de los crímenes cometidos en el entorno digital.
- Los vestigios y la preservación de los datos obtenidos en la investigación del delito.
- La legislación que cubre la práctica de los delitos cibernéticos.
- El proceso de investigación. Y
- Finalizamos con el análisis de un caso concreto de investigación.

Deseamos que este curso haya colaborado en el desarrollo de tus habilidades.

Fue un placer compartir este proceso contigo.

Referencias

BARRETO, A. G.; BRASIL, B. S. **Manual de Investigação Cibernética à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016.

BEDINELLI, T.; MARTÍN, M. Baleia Azul: o misterioso jogo que escancarou o tabu do suicídio juvenil. **El País**, 2 maio 2017. Disponível em: https://brasil.elpais.com/brasil/2017/04/27/politica/1493305523_711865.html. Acesso em: 15 jul. 2020.

BRASIL. [Constituição de 1988]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 15 jul. 2020.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.830, de 20 de julho de 2013.** Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014.** [Marco Civil da Internet]. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2020.

BRASIL. **Decreto n.º 3.810, de 2 de maio de 2001.** Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm#:~:text=Promulga%20o%20Acordo%20de%20Assist%C3%AAncia,15%20de%20fevereiro%20de%202001. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 jul. 2020.

BRASIL. **Lei n.º 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9613.htm. Acesso em: 16 jul. 2020.

BRASIL. **Lei n.º 10.703, de 18 de julho de 2003.** Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.703.htm. Acesso em: 16 jul. 2020.

BRASIL. **Lei n.º 11.340, de 7 de agosto de 2006.** Brasília, DF: Presidência da República, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 16 jul. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. Brasília, DF, 2020. Disponível em: www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/orientacoes-por-pais. Acesso em: 14 jul. 2020.

FLATICON, 2020. Disponível em: https://www.flaticon.com/br/. Acesso em: 16 jul. 2020.

JORGE, H. V. N. **Investigação criminal tecnológica.** 1. ed. Rio de Janeiro: Brasport, 2018. v. 1 e 2.

PEREIRA, M. T. M. A. **Investigação Policial de Crimes Eletrônicos.** São Paulo: Ed. Acadepol, 2019.

PIXABAY, 2020. Disponível em: https://pixabay.com/pt/. Acesso em: 16 jul. 2020.

TIMEBIE. [*S.l.*], 2020. Disponível em: www.timebie.com/timezone/universalbrasilia.php. Acesso em: 15 jul. 2020.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC). Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 14 jul. 2020.

WORLDTIMEBUDDY. [*S.l.*], 2020. Disponível em: www.worldtimebuddy.com/utc-to-gmt-converter. Acesso em: 15 jul. 2020.