



Guía práctica para Investigaciones en entornos digitales

Desarrollada para obtener y comprender la evidencia digital que almacenan las proveedoras de servicio de comunicaciones extranjeras y locales.

UFEDyCI

UNIDAD FISCAL ESPECIALIZADA EN DELITOS
Y CONTRAVENCIONES INFORMÁTICAS

Juan Pablo Delord
Cristian Fariña

Introducción

La realización de ésta guía nació por el constante interés de los operadores del sistema de justicia (jueces, fiscales e investigadores), de conocer qué tipo de información resguardan las empresas que administran cuentas de correos, redes sociales u otras plataformas radicadas en el extranjero, en su mayoría en los Estados Unidos, y de qué modo se la puede solicitar.

En esa línea se buscará facilitar a los operadores de la justicia y sus auxiliares una guía práctica para obtener y comprender la evidencia digital que almacenan las proveedoras de servicios de comunicación a través de Internet radicadas en el extranjero y en el ámbito local, como así también, como es que a través de su análisis se puede instruir una investigación eficiente.

El trabajo pretenderá hacer foco, en la faz práctica de la investigación, sin perjuicio de lo cual, se pondrá a disposición material que permitirá conocer como es la situación jurídica actual en torno al acceso por parte de las autoridades judiciales de un país determinado a datos alojados en extraña jurisdicción a través de la cooperación de las empresas proveedoras de servicios en Internet.

El desarrollo de la guía ha sido realizado por investigadores de la *Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas¹ (UFEDyCI) del Ministerio Público Fiscal de la Ciudad de Buenos Aires* teniendo en cuenta la experiencia que el equipo de trabajo tiene con las empresas que resguardan evidencia digital.

¹ A través de la Res. FG 20-20 suscripta por el Dr. Juan Bautista Mahiques se creó la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas de la Ciudad Autónoma de Buenos Aires.

Pautas Generales

¿Qué tipo de información resguardan empresas como Facebook, Instagram, WhatsApp, Google, Twitter, Microsoft, Yahoo y cómo la podemos obtener?

Como primera medida debemos saber que la información que resguardan estas empresas en reglas generales se divide en:

- **Información básica o de suscripción del usuario**
- **Información transaccional**
- **Información de contenido**

Éste orden surge de la clasificación que las leyes norteamericanas determinan de acuerdo el mayor o menor nivel de intromisión en la privacidad del usuario y, en consecuencia, cuanto mayor sea el grado de intromisión en la privacidad, mayores recaudos deberán cumplirse para obtener la información que se pretende.

Veamos entonces qué tipo de datos abarca cada nivel de información y, en reglas generales como pueden ser solicitados.

Información básica o de suscripción del usuario

- Nombre, país, dirección, teléfonos, edad, género, fecha de nacimiento.
- Cuenta de correo electrónico o número de teléfono asociado.
- Número de tarjeta de crédito.
- Fecha de creación e IP desde la que se creó la cuenta.

Habitualmente esa información es entregada a las autoridades locales a través de los canales directos o informales conocidos como *“Portales para los agentes de la Ley y Fuerzas de Seguridad”*, sin la realización de un exhorto internacional. Algunas firmas cuentan con **portales o plataformas para las fuerzas de la ley** que ellos mismos administran y otras lo hacen a través de **casillas de correo electrónico**. Más adelante detallaremos los requisitos que exige cada empresa.

Se destaca que éste tipo de información puede ser requerida directamente por el fiscal, sin ningún tipo de intervención jurisdiccional.

Información transaccional

Este tipo de información se encuentra comprendida por los datos de remitente y receptor de un correo electrónico, como así también las direcciones IP involucradas en la comunicación, los días y horas en que las comunicaciones se realizaron, la cantidad de datos que insumió, como así también los sitios webs visitados.

Asimismo, se considera información transaccional los registros de conexión del usuario, puesto que estará compuesto con detalle de cada evento de *log in* y *log out* del usuario, especificado con dirección IP, fecha y hora. De su análisis posterior se podrá establecer el sitio exacto en que tuvo lugar cada evento.

Como se advierte a simple vista, el grado de intromisión aquí es mayor, por lo que éste tipo de información y cualquier tipo de pedido de ésta índole, deberá ser materializado con la intervención judicial correspondiente para garantizar los derechos de quien resulte investigado.

Para este tipo de solicitudes, gran parte de las empresas exigen la firma del juez del caso y reciben los pedidos a través de sus portales o vía correo electrónico y, otras empresas exigen el trámite a través de un **exhorto internacional**, lo que garantizará la intervención de autoridades judiciales del país extranjero.

Información de contenido

Éste tipo de información comprende:

- Contenido de texto y adjuntos de correos electrónicos que obren en las carpetas del usuario (entrada, salida, borradores, papelera, etc...)
- Contenido de texto y adjuntos de intercambios en plataformas de mensajería o redes sociales.
- Contenido de publicaciones en redes cuyo acceso se encuentra restringido.
- Historial de localización del usuario.
- Fotos y otros documentos almacenados en la nube.

La información de contenido necesariamente debe ser requerida a través de un **exhorto internacional**, puesto que el grado de injerencia en la privacidad del usuario es aún mayor.

Debemos saber que cuando la evidencia digital se encuentra en el exterior, el mecanismo previsto entre los Estados para obtener dicha evidencia se rige por las normas de cooperación internacional.

Fundamentalmente hay dos caminos a seguir:

- a. exhortos internacionales o,
- b. tratados de asistencia legal mutua (MLAT), acordados entre países.

La práctica demuestra que este canal de comunicación entre diferentes países en cuanto a la evidencia digital no es tan eficiente como se supone debe ser, y para cuando el país requerido analiza el MLAT, es posible que la evidencia digital ya no exista y/o haya migrado a otro servidor, en otro país. Ni hablar en

aquellos casos donde no existe entre los países un acuerdo de asistencia legal mutua y deben recurrir inevitablemente a un exhorto internacional.

En el ámbito local, ha sido la Ley 24.034, la que aprobó el Tratado de Asistencia Mutua en Asuntos Penales con el Gobierno de Estados Unidos, con el objeto de intentar mejorar la eficacia en las investigaciones mediante la cooperación y asistencia mutua.

El acuerdo prevé un mecanismo que aspira a lograr una comunicación más ágil a la hora de requerir información alojada en el país extranjero, aunque

Sintéticamente podemos decir que se trata de un trámite complejo y extenso que involucra muchos actores y demora aproximadamente unos de diez (10) meses. Ello, en caso de que todas las revisiones a las que es sometido el trámite por los distintos estadios fuesen exitosas.

Como se advierte, el mecanismo requerido por el MLAT es sumamente lento y no está a la altura del rápido desarrollo de la tecnología y su correlativa necesidad de una intervención rápida y eficaz por parte de las autoridades judiciales frente a la comisión de un delito.²³

² Dupuy D., Kiefer M., “La transferencia transfronteriza de datos en el marco de investigaciones criminales” Revista Derecho y Nuevas Tecnologías, Número 2. CETyS. Dir.: Palazzi P., Universidad de San Andrés, Autoría: Dupuy, Daniela Mariana Kiefer, 2020.

³ Dupuy d., Kiefer M., “Datos e innovación tecnológica” en Cibercrimen III, Dir. Dupuy D. y Corvalán J. y Coor. Kiefer M., Ed. BdeF, Buenos Aires (2020), pág. 353-396.

Conservación de la Información

Cuando desarrollamos investigaciones en entornos digitales debemos saber que cualquiera sea el tipo de información que pretendamos, la misma puede ser eliminada, ya sea por políticas de la propia empresa, como así también, por parte del propio usuario. Por eso es fundamental poder conservarla de modo rápido hasta el momento de solicitarla.

Muchas veces, quien comete alguna maniobra delictiva a través de medios digitales, procura mantenerse impune, borrando todo tipo de rastros que permitan su identificación.

Entonces, si los encargados de la investigación y conservación de la evidencia llegamos a tiempo, podemos requerir a las empresas proveedores de servicios la conservación de datos, para que al momento de diligenciar el pedido formal de la información –ya sea a través de un oficio judicial diligenciado por canales directos o exhorto internacional- la empresa requerida cuente con la información básica, transaccional o de contenido que se pretende.

Se trata de un procedimiento sencillo que no comprende una medida probatoria, sino que tiene naturaleza cautelar y que permitirá **conservar la información por un lapso de 90 días hasta el momento de realizar la petición formal**, evitando de esta manera que la información se pierda antes de ser incorporada al proceso.

Para que las peticiones de conservación se hagan efectivas, es necesario la existencia de elementos objetivos que permitan sospechar de una actividad ilícita y su relación con la información que se pretende conservar y; el peligro en la demora.

Casos de emergencia

En casos de emergencia las empresas proveedoras de servicios pueden entregar voluntariamente información básica, transaccional o de contenido del usuario sin la necesidad del diligenciamiento de un exhorto internacional. Se trata de una medida de excepción denominada *Emergency Disclosure Request*.

Para obtener la información deberá demostrarse que la existencia de una emergencia que involucre riesgo de muerte inmediato o de seria afectación a la integridad física de una persona, de modo que se requiere contar con la información sin demora. Para ello, al momento de la petición se deberá fundar detalladamente la urgencia de la medida e inclusive se podrá acompañar prueba que sustente la petición.

Son pedidos que se realizan de modo directo a las empresas proveedoras de servicios, cuyas autoridades evaluarán si el supuesto planteado se ajusta a un caso de emergencia o si será desestimado. La cooperación es voluntaria.

¿Qué tener en cuenta para realizar un pedido de información a una empresa radicada en el extranjero?

Si bien al inicio se ha hecho referencia al tipo de información que resguardan las empresas que administran redes sociales, servicios de mensajería instantánea o de correos electrónico (Información básica o de suscripción del usuario, transaccional o de contenido y las exigencias –en términos generales– que la norma americana prevé para proveernos de dicha información) no debemos perder de vista que dicha clasificación ha sido determinada a la luz de una ley extranjera, razón por la cual, no podemos perder de vista en ningún momento las leyes locales y las garantías procesales que debemos respetar en toda investigación penal.

Entonces, resulta fundamental explicar qué entendemos por datos de abonado, tráfico y contenido, conforme las leyes e interpretaciones locales y qué cuestiones tener en cuenta para que dicha información se agregada al Legajo sin cuestionamientos.

- **Datos de abonado:** Es la información que posee una empresa proveedora de servicios relacionada con los abonados de sus servidores (identificación, dirección, n° de teléfono, datos de facturación, pago, lugar físico de conexión).
- **Datos de tráfico:** Es la información sobre el circuito de una comunicación realizada por medio de un sistema informático: origen, destino, ruta, hora, duración y fecha de la comunicación.
Son los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elementos de la cadena de comunicación y que indique el origen y el destino, la ruta,

la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

- o **Datos de contenido:** Son los que permiten determinar la información intercambiada por las partes que intervinieron en la comunicación (por ejemplo el contenido de una conversación de voz por IP, el contenido de un correo electrónico, un mensaje privado de Twitter o Facebook, conversación de WhatsApp, etc.)

Debemos tener en cuenta que la clasificación expuesta es importante, puesto que implica distintos grados de injerencia en la esfera de intimidad de las personas.

El mayor inconveniente se presenta cuando intentamos determinar si los datos de abonado, de tráfico y de contenido se encuentran amparados por las mismas garantías fundamentales como el derecho a la intimidad y privacidad, o si se trata de distintos grados de intromisión a la esfera de intimidad de las personas que tiene permitido el poder estatal.

Por eso cuando se realice la petición a una empresa radicada en el extranjero se deberá evaluar, teniendo en consideración el tipo de información que se solicita –de abonado, tráfico o contenido- si la misma debe ordenarse por parte del Juez (como garante de los derechos fundamentales del investigado) o, si en su caso podrá ser el Fiscal quien realice directamente el pedido. Ello, sin perjuicio de las formalidades propias que cada empresa extranjera requiera.⁴

⁴ Neme, Catalina UNA MIRADA ACTUAL EN MATERIA DE REGULACIÓN DE RETENCIÓN DE DATOS DE TRÁFICO y CONSERVACIÓN RÁPIDA DE DATOS INFORMÁTICOS”, en Ciberdelincuencia I, Dir. Dupuy D. y Coord. Kiefer M., Ed. BdeF, Buenos Aires (2017), pag 407-439.

Pautas generales sobre Investigaciones en entornos digitales

Adentrándonos en el objetivo concreto de ésta Guía, en primer lugar se explicarán una serie de conceptos y definiciones propias de las investigaciones en entornos digitales, que permitirán lograr una correcta interacción con las empresas radicadas en el extranjero, como así también una correcta interpretación de la información que esas empresas nos suministren.

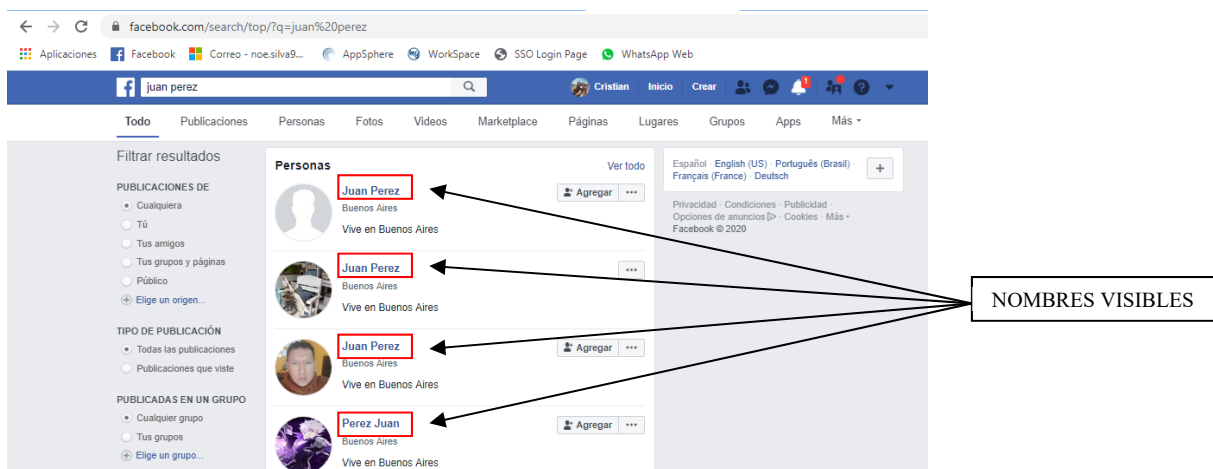
¿Cómo identifico un usuario de una red social, plataforma de mensajería instantánea o cuenta de correo electrónico?

Muchas veces hacemos referencia a un usuario a través del nombre visible del usuario en las redes, sin embargo, debemos saber que el nombre visible a simple vista no resulta útil para realizar peticiones a las empresas proveedoras de servicios, puesto que es probable que existan usuarios homónimos y que además la empresa a la que se hace el pedido exija que el usuario consultado sea identificado mediante un dato único e irrepetible.

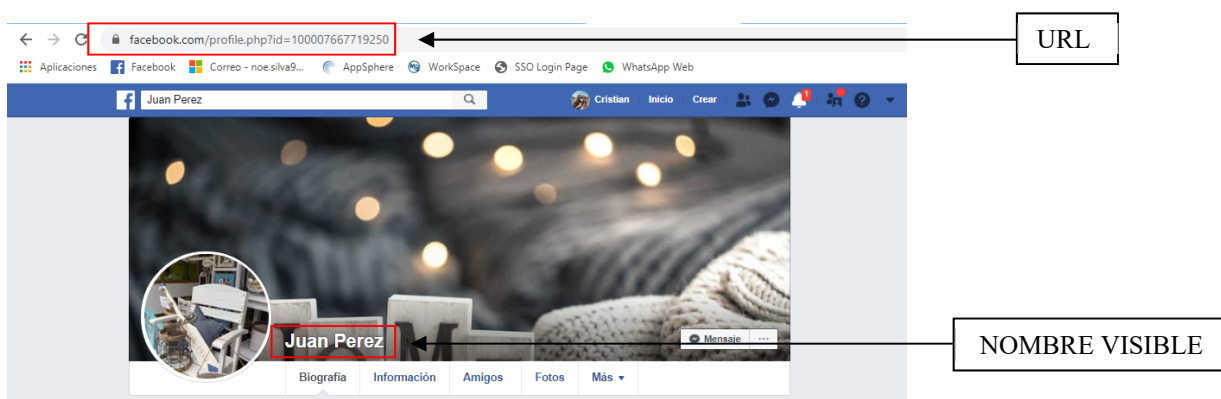
Por esa razón la forma más efectiva de identificar un perfil en una red social a través de la URL⁵ que genera el sitio al momento de observar la página de inicio del perfil investigado. Veamos algunos ejemplos.

⁵ URL es una sigla del idioma inglés correspondiente a Uniform Resource Locator (Localizador Uniforme de Recursos). Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados.

Facebook



Como se observa, para la búsqueda “Juan Perez”, la plataforma arroja múltiples resultados homónimos. Por tal motivo el usuario investigado debe ser identificado como se indica a continuación.

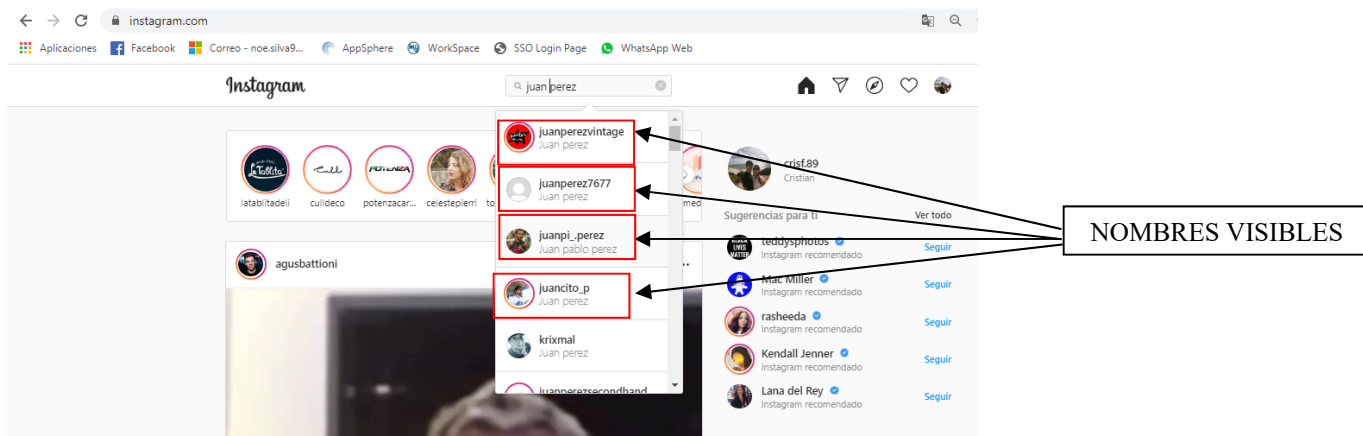


URL: <https://www.facebook.com/profile.php?id=100007667719250>

ID 100007667719250

Asimismo, en caso de querer conocer cuál es la ID del usuario, accediendo al sitio <https://es.piliapp.com/facebook/id/> y transcribiendo la URL completa del perfil se obtiene la ID del usuario que en este caso sería: **100007667719250**

Instagram



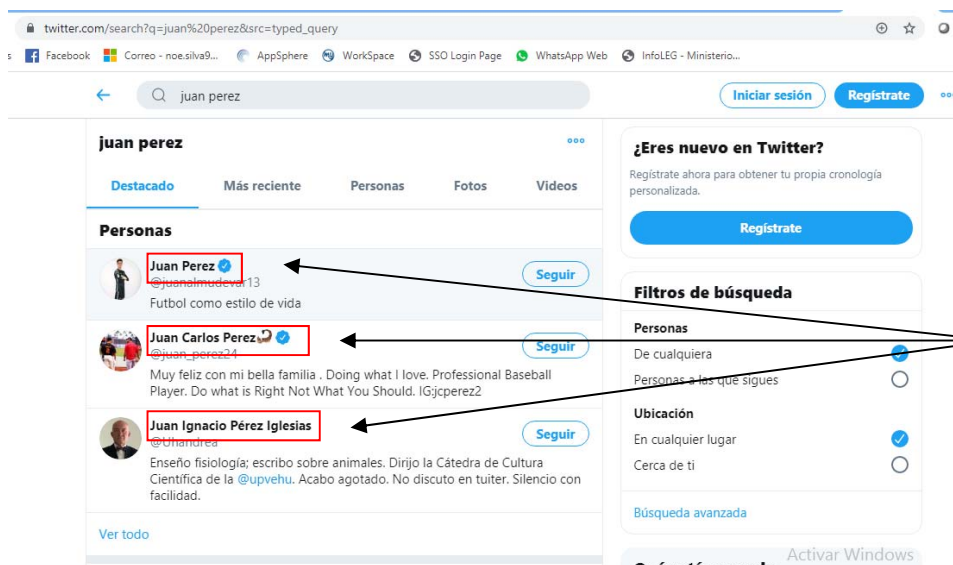
Aquí también, vemos como ante una búsqueda bajo el parámetro “Juan Perez”, la plataforma arroja múltiples resultados. Para las investigaciones digitales la correcta identificación debe realizarse como se indica a continuación.



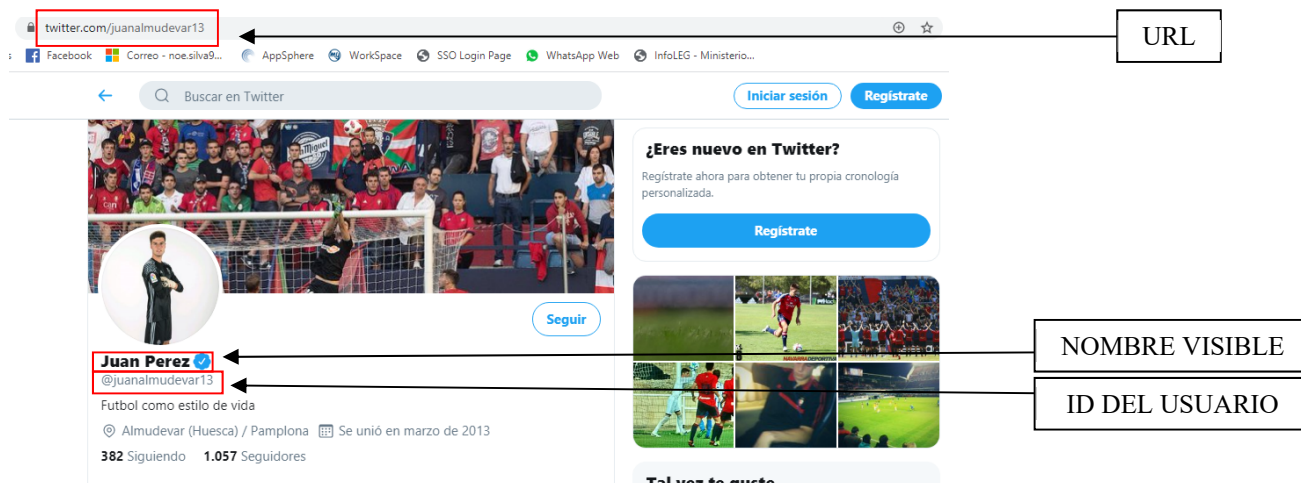
URL http://www.instagram.com/juancito_p

ID juancito_p

Twitter



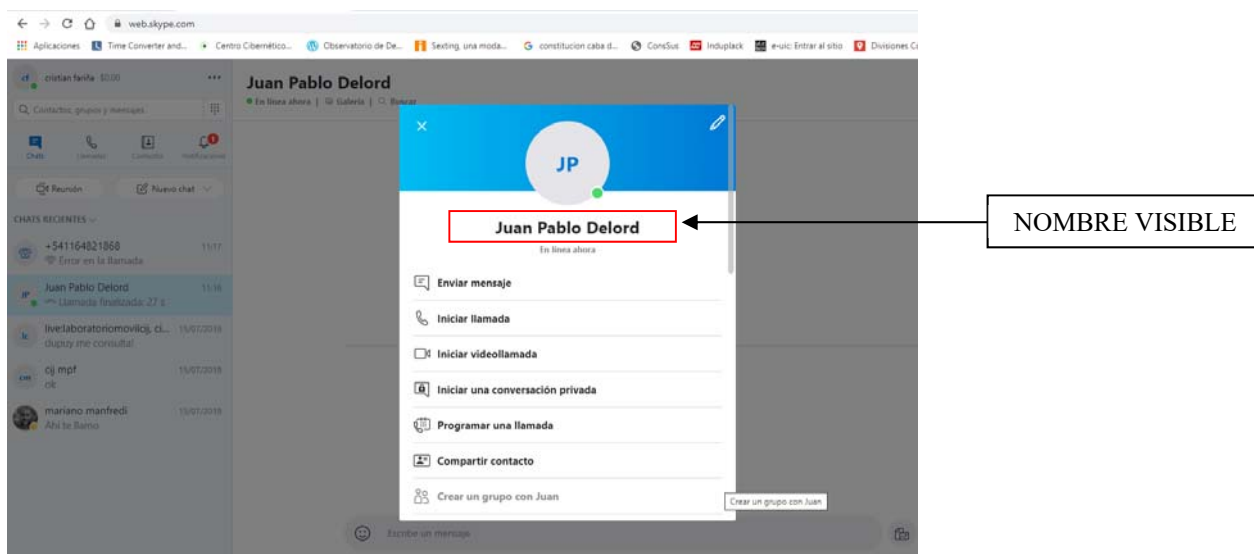
De igual manera que en casos anterior la identificación de un determinado usuario a través de su nombre visible ofrece múltiples resultados. Por tal motivo, quien resulte objeto de investigación deberá ser individualizado a través de la URL del perfil o en su caso a través de su ID.



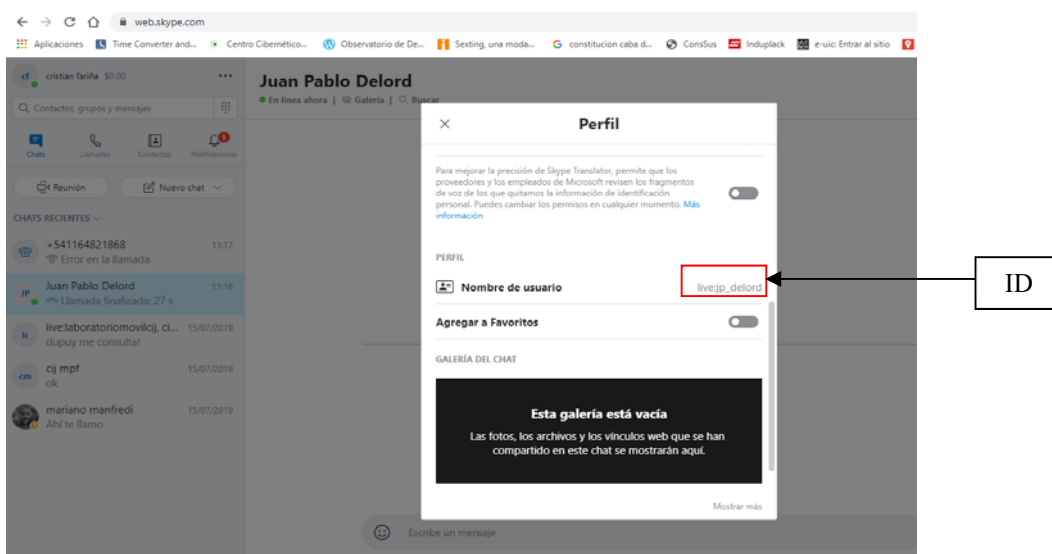
URL <http://www.twitter.com/juanalmudevar13>

ID @juanalmudevar13

Skype

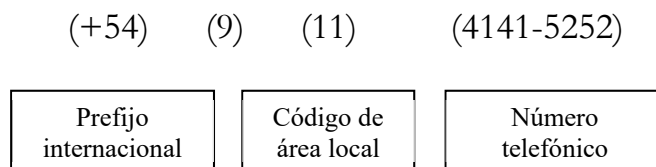


Si lo que estoy investigando es un usuario de Skype, la identificación correcta debe realizarse accediendo a los datos del perfil del usuario. Como se observa en este caso, el nombre visible es “Juan Pablo Delord”, pero la correcta identificación a través de su **ID** es: **live:jp_delord**



¿Cómo identifico un usuario de WhatsApp?

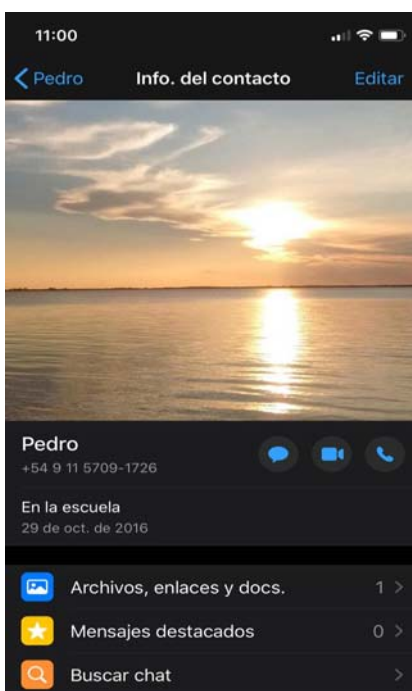
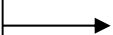
Será identificado a partir del número de abonado telefónico que posea el usuario que deberá ser descripto con del modo que a continuación se detalla



Debemos tener en cuenta que el prefijo internacional sólo indicará el país de origen de la línea telefónica vinculada a WhatsApp, pero de ningún modo ese dato determina que el usuario se encuentra en el país al que corresponde el prefijo.

De éste modo, podemos estar un investigando un sospechoso con prefijo internacional distinto al argentino (+54), pero sin embargo, si dicho usuario está llevando a cabo su maniobra en territorio Argentino, podremos consultar a la firma WhatsApp los datos de registración y de conexión de ese usuario. Más adelante detallaremos cómo.

ID de usuario de WhatsApp



¿Cómo identifico el usuario de una cuenta de correos?

En estos casos la identificación es más simple, debido a que las empresas proveedoras de servicios de correo electrónico no permiten cuentas correos duplicadas. Sólo debemos tener en cuenta que algunas firmas poseen varios dominios lo que permitirá dirigir correctamente el pedido de conservación e información del usuario, como así también que algunas cuentas finalizan como **.com** y otras **.com.ar**.

Google	<u>juanperez@gmail.com</u>
Microsoft	<u>juanperez@hotmail.com</u>
	<u>juanperez@live.com</u>
	<u>juanperez@outlook.com</u>
Yahoo	<u>juanperez@yahoo.com</u>
	<u>juanperez@yahoo.com.ar</u>

¿Qué es una dirección IP?

La dirección IP –*Internet protocol*– es un conjunto de números que identifica de manera lógica y jerárquica, a una Interfaz en red de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

En términos sencillos, podemos decir que la empresa proveedora del servicio de Internet (Cablevisión, Telefónica, Telered, Telecentro, Claro, etc...) asignará una IP determinada a cada cliente para que, a través de ella, tenga

conectividad a Internet. Esa IP puede ser fija o dinámica, pública o privada. Veamos.

-IP pública: es aquella que identifica de forma única una conexión a Internet.

-IP privada: es aquella que se utiliza única y exclusivamente en redes de área local que no pueden salir a navegar por Internet.

Dependiendo el tipo de conexión o empresa que provee el servicio de Internet la dirección IP puede ser:

-IP fija o estática: en éste caso el cliente se conectará siempre con la misma dirección IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet.

-IP dinámica: en este caso cada vez que el cliente se conecte a la red lo hará mediante una dirección IP dinámica, es decir, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas, son las que se utilizan en las conexiones de Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas porque tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Tanto el tipo de IP dinámica o fija son los utilizados usualmente para redes domésticas y gran parte de las empresas que proveen servicios de Internet guardan registros de asignación de IP, lo que permitirá conocer qué cliente y desde que sitio de instalación del servicio se conectó a esa IP.

¿Cómo identifico una IP?

Sin adentrarnos profundamente en cuestiones técnicas, podemos decir que una dirección IP es un conjunto de números, cuyas combinaciones posibles son finitas.

Tal circunstancia ha generado la necesidad de crear distintos tipos de IP para lograr abastecer la demanda de conectividad que exigen los usuarios.

Veamos algunos ejemplos de tipos de IP's que nos podemos encontrar en una investigación.

IPv4	190.193.157.7
IPv6	2001:0db8:85a3:08d3:1319:8a2e:0370:7334

¿Qué se entiende por Nateo de IP?

El nateo de IP es utilizado para que, a través de una dirección IP pública se pueda proveer conectividad a gran cantidad de usuarios por intermedio de diferentes IP privadas.

Esta modalidad de prestación del servicio es la utilizada en gran medida por las empresas prestarias de servicio de Internet móvil y así lograr la gran demanda de los usuarios. Si bien es una solución eficaz, desde el punto de vista la investigación suele ser un obstáculo, debido a que las empresas no suelen contar con registros de asignación histórica por Nateos, amparados claro, en que hoy día no hay normativa alguna que los obligue a guardar esos datos.

¿Qué es un huso horario?

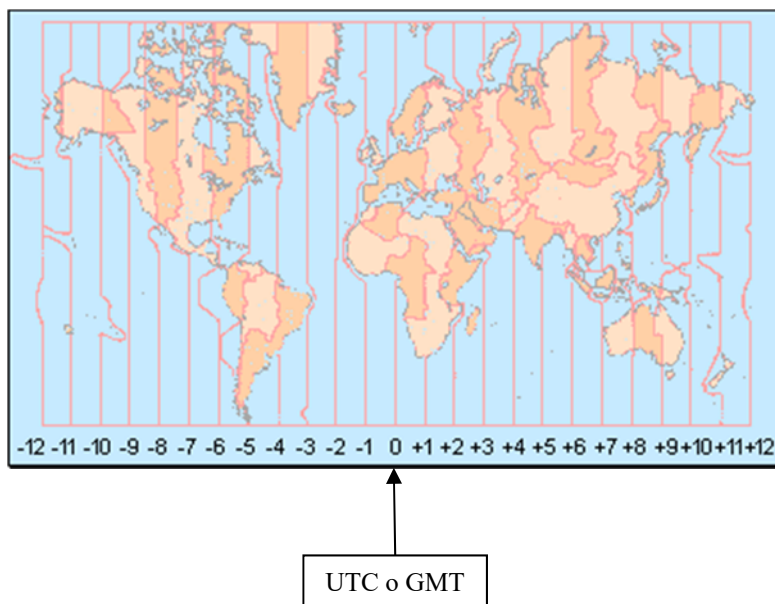
¿Cuál es su importancia?

Teniendo en consideración que la información relativa a fechas y horas que proveen las empresas radicadas en el extranjero, se detalla en husos horarios diferentes al argentino, es imprescindible comprender cuál es su definición, como así también de qué modo se realizan conversiones horarias correspondientes.

Ello es esencial, puesto que luego de convertir la información remitida por las empresas extranjeras, se cursarán consultas a empresas locales que resguardan los datos relativos a conexiones en huso horario local. Cometer un error en la conversión horaria puede generar el fracaso de la investigación.

Pasando entonces a su definición, podemos decir que un huso horario es cada una de las 24 áreas en que se divide la Tierra por un meridiano y, en la que rige por convención el mismo horario. Ello implica que en un momento determinado, en husos horarios diferentes, un evento se registra en distintos horarios y para ello debemos aprender a realizar conversiones horarias sin cometer errores. Un error en etapa de la investigación puede direccionar pesquisa hacia sitios o domicilios de conexión erróneos.

Resumiendo, resulta trascendental adquirir estos conocimientos, puesto que las empresas radicadas en el extranjero proveen su información relativa a fechas y horas, en husos horarios distintos a los utilizados en Argentina. Lo mismo sucederá en países que utilicen husos horarios distintos a aquellos utilizados por las empresas proveedoras de servicios de comunicación.



Tal como se observa en la imagen, todos los husos horarios se definen en relación con el denominado tiempo universal coordinado (*United Time Cordinated*), huso horario centrado sobre el meridiano de Greenwich (también conocido como meridiano cero o por sus siglas en inglés GMT *Greenwich Mean Time*).

Puesto que la Tierra gira de Oeste a Este, al pasar de un huso horario a otro en dirección este, hay que sumar una hora. Por el contrario, al pasar de Este a Oeste hay que restar una hora; y es el meridiano de 180° el que marca el cambio de día.

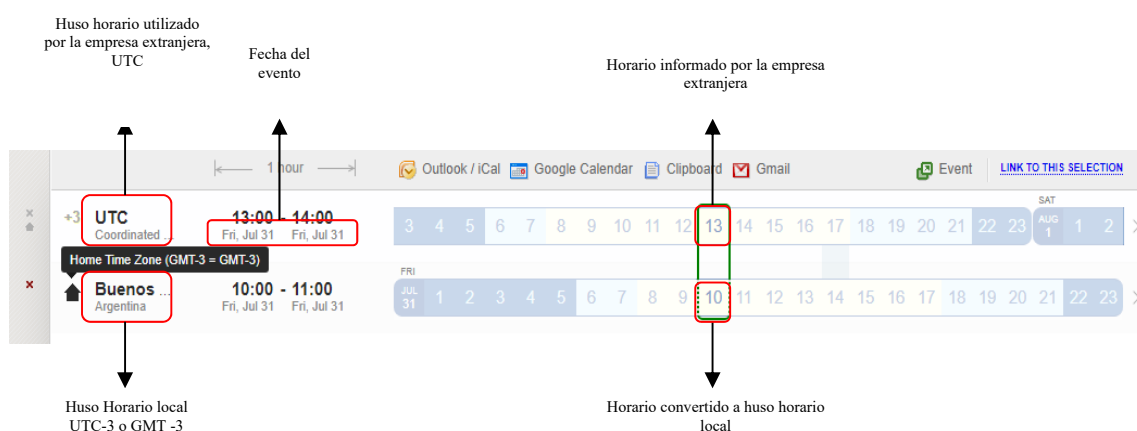
Por norma general, los países siguen esta regla, sin embargo, en algunas partes del mundo, los relojes se han cambiado dejando horarios diferentes, inclusive algunos varían su huso horario de acuerdo al momento calendario del año, razón por la cual, recomendamos que las conversiones horarias se realicen a través de sitios actualizados y dedicados exclusivamente a ello.

Debemos tener en cuenta que cada empresa proveedora de servicios – Facebook, Microsoft, Google, Yahoo, etc... provee información en husos

horarios diferentes, siendo los más utilizados los husos UTC, GMT, PDT, EST, EDT que luego serán cotejados con el huso horario argentino **UTC -3** o el huso local del país donde se desarrolla la investigación.

Será tarea del investigador convertir el evento informado por la empresa extranjera al huso horario utilizado en Argentina (UTC-3). Es decir, el territorio Argentina se encuentra a tres horas menos del huso UTC. De modo que, si en el Huso UTC son las 13:00 horas en territorio argentino serán las 10:00 horas.

Ahora bien, para que la conversión de los husos sea precisa, toda vez que la diferencia horaria puede variar en distintos momentos calendario del año, recomendamos la utilización del sitio: <https://www.worldtimebuddy.com/>. Allí se deberán consignar los dos o más husos horarios a consultar, la fecha y la hora del evento y de esa manera, obtendremos la conversión correcta.



Al momento de utilizar el sitio propuesto, como primera medida debemos indicar el día mes y año del evento y luego elegir los distintos Husos horarios que deseo corroborar. De esta manera, se obtendrá cual es la diferencia horaria para ese momento del año, al tiempo que permitirá movernos por toda la franja horaria de ese día.

Como se observa en la captura, para el día 31 de julio de 2020, se seleccionó el huso horario UTC o GMT (Huso horario 0) por un lado y, por otro, se seleccionó la localidad Buenos Aires o Huso horario UTC-3 o GMT-3 de modo tal que si en UTC 0 son las 13.00 horas; en UTC-3 son las 10.00 horas.

¿Qué es un *log* o registro de conexión y cómo se compone?

En informática, se usa el término *registro, log o historial de log* para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).

De esta forma, un log de creación, registración o conexión de un usuario de determinado sistema, constituye una evidencia del comportamiento y, a través de su análisis posterior se podrá determinar el sitio y momento exacto desde donde se produjo ese evento.

Un *log o registro* se compone de una dirección IP y de la fecha hora en que el mismo tuvo lugar, con indicación del huso horario en que está siendo informado.

Normalmente ante las requisitorias efectuadas, las empresas extranjeras informan los logs de la siguiente manera.

Google

Time	IP Address	Type
2019/06/20-00:05:36-UTC	181.90.252.176	Login
2019/06/20-00:05:35-UTC	181.90.252.176	Login
2019/06/12-04:20:17-UTC	181.118.73.53	Login

Fecha en formato AÑO/MES/DIA
 Hora del evento
 Huso Horario
 Dirección IP

Facebook/Instagram/WhatsApp

IP Address 186.141.202.208
Time 2018-03-10 23:31:04 UTC

IP Address 186.141.134.196
Time 2018-03-09 18:53:50 UTC

IP Address 186.141.197.65
Time 2018-03-09 17:34:53 UTC

Microsoft

Query for: ciudadmadero22@hotmail.com.ar
 Date Range: 1/1/1990 12:00:00 AM to 6/11/2018 11:59:59 PM

Record Type (Registration)	Signin Name	First Name	Last Name	Region / State	Postal Code
Registration Profile	ciudadmadero22@hotmail.com.ar	guillermo	madero	Buenos Aires	1150
Record Type (IP Connection History)	Last Modified Date and Time	Action	IP Address		
IP Connection History	5/22/2018 12:44:40 PM	Login Success	152.168.9.85		

All times are captured in UTC (GMT), and the time-stamps come from the MSA servers and not the user's computer.

Report Created: 6/22/2018 5:29:04 AM

IP Activity for 1/1/1990 to 6/11/2018 for account: ciudadmadero22@hotmail.com.ar (UTC Time)

Mailbox	Client IP address	Access Time
ciudadmadero22@hotmail.com.ar	201.252.14.57	02/12/2010 16:13:51
ciudadmadero22@hotmail.com.ar	181.30.248.22	14/01/2018 21:00:16
ciudadmadero22@hotmail.com.ar	2800:2141:3000:d5:8075:87d8:14f2:7cf6	13/03/2018 19:58:17

*Currently our system is not collecting the IP address for some log-ins. These log-ins are being released with the date and time, to show account activity.

→ Telecom Argentina S.A.
 → Telecom Argentina S.A.

¿Qué puedo obtener a raíz del análisis de esa información?

Permitirá establecer el sitio físico de conexión de cada evento informado por las empresas proveedoras de servicios de comunicación -Google, Facebook, Instagram, etc...-, verificando de esta manera cuál es el comportamiento del usuario investigado.

Sin embargo, la sola lectura de los registros difícilmente permita obtener algún dato de interés para la investigación, de modo tal que, será tarea del investigador determinar qué empresa es la que administra y pertenece la dirección IP informada. Para ello recomendamos el uso del sitio público de consultas www.iplocation.net o rdap-web.lacnic.net/y, una vez obtenida esa información, se requerirá a esa empresa a qué usuario o cliente de su compañía asignó la IP consultada en la fecha y hora informada por las empresas como Google, Facebook, Microsoft etc.

Una vez realizada la búsqueda en el sitio se exhiben los resultados de la siguiente manera:

The screenshot shows the RDAP Web client interface. At the top, it says 'RDAP Web client' and 'Inicio'. On the right, there are language options: 'Español | English | Português'. The main content area is divided into two sections: 'IP' and 'CONTACTS'. The 'IP' section shows details for the IP 186.136.171.110, including its handle (186.136.0.0/15), status (allocated), net range (186.136.0.0 - 186.137.255.255), net version (v4), registration date (2009-04-17T17:21:11Z), and last changed date (2018-05-29T20:17:17Z). The 'CONTACTS' section shows the registrant as 'Telecom Argentina S.A.' with a telephone number (54 11 49684975) and links for more info and source. A red box highlights the IP address in the search area, and another red box highlights the registrant name 'Telecom Argentina S.A.' in the contacts section. Arrows point from these boxes to explanatory text below.

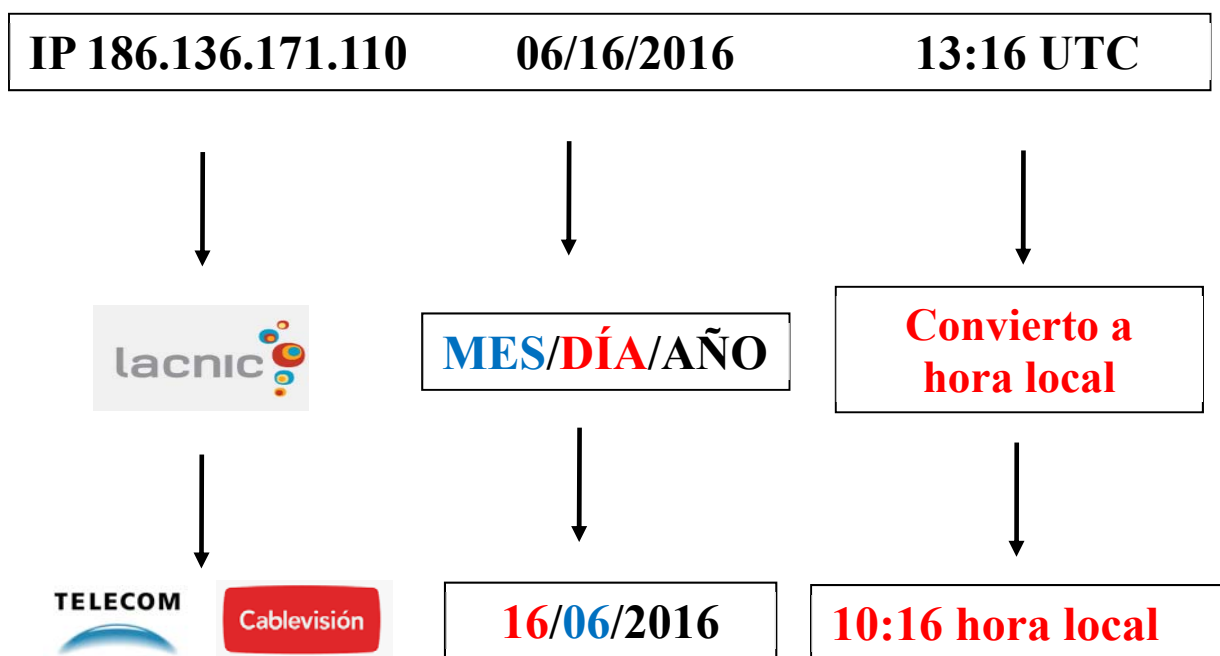
En el panel de búsqueda se deberá consignar la IP que se desea consultar. Se pueden consultar interfaces del tipo IPv4 o IPv6

El dato de mayor interés en la consulta es la ISP (Internet Service Provider) en donde se consigna qué empresa es la que administra la IP consultada.

Posteriormente se deberá consultar a la ISP –*Internet Services Provider*- a qué cliente o usuario de su compañía le fue asignada la IP en la fecha y hora – convertida al huso horario local-, que fue oportunamente informada por las empresa proveedoras de servicios extranjera.

Reunida esa información se podrá determinar el lugar físico de conexión del usuario investigado conforme el listado de logueos o de conexión informado por Google, Facebook, Instagram o la empresa que corresponda.

Resumiendo, el análisis podrá sintetizarse de la siguiente manera:



De esta manera una vez, determinada la empresa y la fecha y hora correcta del log de conexión será momento, de consultar a la firma proveedora del servicio de Internet, en este caso Telecom/Cablevisión, que informen a que cliente de su compañía se encontraba asignada la IP 181.16.268.36 el día 16/02/2015 a las 12:35 hora local.

A través del link <http://icannlac.org/PO/isps-ar> se podrán consultar los datos de contacto de todas las empresas argentinas prestatarias de servicios de

Internet, entre las que se observan a modo ejemplo: Cablevision, Telefónica de Argentina, Nextel, Movistar, Personal, AMX Claro, Telecentro, ARSAT, Teledifusora S.A., Eurosat, Direct Tv Argentina. En dicho listado se podrán consultar un total de 348 empresas prestatarias de servicios de internet registradas ante Lacnic, constando además los links o datos de contacto de cada una de ellas.

Seguidamente, obtendremos una respuesta como la que a continuación se detalla:

Gral. Hornos 690 - C1272ACL - Ciudad Autónoma de Buenos Aires
Argentina
LegalesOficios@cablevision.com.ar

Buenos Aires, 9 de junio de 2017

MINISTERIO PUBLICO FISCAL DE LA CIUDAD AUTONOMA DE BUENOS AIRES
Unidad de Análisis e Investigación Tecnológica del Cuerpo de Investigaciones Judiciales.

Tuyu N° 86
Ciudad Autónoma de Buenos Aires.
S_/_/___D

De mi mayor consideración:

Tengo el agrado de dirigirme a U.D. en respuesta al oficio librado en el marco del caso **NCMEC N° 12520864** caratulado **"NN s/infracción al art. 128 del C.P. - PRODUCIR, FINANCIAR, OFRECER, COMERCIAR, PUBLICAR, FACILITAR, DIVULGAR O DISTRIBUIR PORNOGRAFIA INFANTIL"**, con el fin de brindar la siguiente información:

EP	FECHA	HORA						
186.136.171.110	16/06/2016	20:16						
NOMBRE	APPELLIDO	IDENTIFICACION	DOMICILIO	TELEFONO	SERVICIO	ESTADO DEL SERVICIO	METODO DE PAGO	E-MAIL
NEVO	GUY		11 DE SEPTIEMBRE 1245 CABA	MOVIL 7111	TV X CABLE HD FIBERTEL 12MEGAS WIFI	ACTIVO 709a 21/11/2012	AMERICAN EXPRESS 19001	guy@gmail.com

Luego de ello serán medidas de investigación en torno al/los domicilio/s obtenido/s, sus moradores y análisis en fuentes abiertas, con el objeto de determinar el sitio de comisión de los hechos y su posible autor.

Solicitudes de información a empresas radicadas en el extranjero

En esta segunda parte, avanzaremos en una minuciosa guía explicativa que dará cuenta de los requisitos y modos en que cada empresa gestiona los pedidos de conservación de datos del usuario y solicitudes de información, cómo deben ser interpretados esos datos y qué otras medidas se pueden adoptar con ellos.

Para ello, se ha realizado una selección de las empresas proveedoras de servicios utilizadas con mayor frecuencia para cometer ilícitos y cuyos procedimientos de conservación de datos y de pedidos de información han sido utilizados y corroborados, sin perjuicio de lo cual se facilitará información de contacto y manuales para la fuerza de la ley de numerosas empresas.

Teniendo en consideración que las empresas radicadas en el extranjero se rigen por la normativa local que a cada una de ellas les comprende, como así también, que cada empresa posee requisitos específicos que determinarán el éxito final de la medida, es sobre ese punto en particular que versará esta parte de la guía.

A continuación se irá avanzando por empresas en los procedimientos de conservación de información y solicitud de información de registro y conexión, precisando los requisitos y exigencias de cada firma.



1. Microsoft -Outlook, Hotmail, , Xbox, , One Drive, Skype

En relación a las peticiones a la firma Microsoft Inc. Las peticiones deberán ser canalizadas a través del portal que la firma pone a disposición de los agentes de la Ley a través de la URL <https://leportal.microsoft.com/home>

Cabe destacar que anteriormente las peticiones a esta firma eran realizadas a través de la cuenta de correos **asklcala@microsoft.com**, la cual desde la implementación del portal, ha quedado en desuso.

Respecto de la utilización del portal, se adjunta a la guía un documento provisto por la propia empresa que detalla de manera pormenorizada los requisitos y pasos a seguir para registrarse en la plataforma y proceder a su utilización.

A modo de síntesis podemos decir que para la registración se necesitará una cuenta con dominio Hotmail, Outlook, Yahoo o Gmail y además una cuenta oficial de trabajo que registre dominio .gob o .gov y con ello se podrá avanzar en la registración del portal.

¿Qué tipo de pedidos se puede realizar a la empresa?

- Conservación de datos de la cuenta investigada
- Solicitud de información de registración y logueo
- Solicitud de información de contenido

¿Qué requisitos debemos cumplimentar para cada tipo de solicitud?

1.1 Solicitud de conservación de cuenta

La petición se hará vía a través del portal <https://leportal.microsoft.com/home> y se deberán completar datos como nombre del agente que realiza el pedido, datos de contacto, servicio de Microsoft sobre el cual se solicita la información –MSA, Skype, Correo electrónico, Xbox, One Drive-, debiendo acompañar además un oficio suscripto por un funcionario judicial (Fiscalía o Juzgado) o en su caso un funcionario policial, cuyos requisitos se exponen a continuación.

- Estar dirigido a:

Legal and Corporate Affairs (LCA)

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052, USA

Fax: 954-492-1976

Dicho oficio deberá contener una descripción del tipo de delito investigado y estar firmado por la autoridad que emite la solicitud, el cual puede ser cualquier funcionario judicial y/o policial, como así también se debe detallar la información específica que se requiere sobre la dirección de correo electrónico o en su caso la conservación de datos.

- Se deberá consignar en el oficio **que la empresa Microsoft Inc. no de aviso a su cliente respecto del pedido solicitado indicando el marco**

legal por el cual no se dará aviso. Por ejemplo, que se trata de una investigación penal en trámite.

A continuación, se detalla un modelo de oficio:

Buenos Aires, 28 de julio de 2020

Legal and Corporate Affairs (LCA)

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052, USA

Fax: 954-492-1976

Tengo el agrado de dirigirme a Ud. por así haberlo dispuesto la titular de la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas, en el marco del caso MPF 1234, caratulado “cuenta-investigada@hotmail.com s/ Infracción Art. 128 Código Penal de la Nación” a fin de que solicitarle realizar la conservación de datos de registro, conexión y contenido de la cuenta de correo, a saber:

cuenta-investigada@hotmail.com

Asimismo, pongo en su conocimiento que la presente investigación gira en torno a una posible infracción al artículo 128 del Código Penal de la Nación que establece: “Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor

de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.”

Se solicita que se evite formular cualquier tipo de notificación al usuario de la cuenta mencionada por tratarse la caso penal en curso y así lograr el éxito de la investigación.

Saludo a Ud. muy atentamente

1.2 Solicitud de datos de registración y logueos

Cuando tengamos que requerir información de registración y conexión de una cuenta de Microsoft, la petición también se hará a través del portal provisto a través de la URL <https://leportal.microsoft.com/home>, debiendo completar los distintos campos que el sistema propone, debiendo adjuntar un oficio solicitando la información en cuestión.

Cabe destacar que la empresa no exige firma de Juez al momento de solicitar estos datos, sino que el oficio puede está firmado directamente por parte del Fiscal. Sin embargo, teniendo en consideración el tipo de información que obtendremos, recomendamos realizar la petición con la intervención judicial correspondiente, en pos de evitar cualquier tipo de cuestionamiento posterior.

Una vez procesado el pedido por parte de la empresa, llegará una notificación que nos avisará que la información se encuentra lista para ser descargada desde el portal.

A continuación, se adjunta un modelo de oficio firmado por una autoridad judicial en el que se solicitan datos de registración y logueo.



2020 Año del General Manuel Belgrano



Buenos Aires, 10 diciembre de 2020.

LEGAL AND CORPORATE AFFAIRS (LCA).

MICROSOFT CORPORATION WAY

REDMOND, WA 98052, USA FAX 954-492-1976

S / D

Tengo el agrado de dirigirme a Ud. en mi carácter de Juez a cargo del Juzgado de Primera Instancia en lo Penal, Contravencional y de Faltas nro.28, sito en la calle Beruti Nro.3345, 3º piso de esta Ciudad (tel/fax 4014-5855) en la causa r [REDACTED]/2020-0 caratulada “**NN, NN SOBRE 128 1 PARR - DELITOS ATINENTES A LA PORNOGRAFIA (PRODUCIR/PUBLICAR IMAGENES PORNOGR. C MENORES 18)**” a efectos de solicitarle los siguientes datos del usuario del correo electrónico [REDACTED]@hotmail.com, que a continuación se detallan:

- 1- Datos de registración del usuario;
- 2- Datos del Registro de direcciones IP utilizadas tanto para la creación como para el acceso hasta el presente, con indicación de las fechas y horas pertinentes;
- 3- Información registrada del usuario;
- 4- Información sobre eventuales cambios de contraseña y;
- 5- Las distintas y/o sucesivas cuentas de correo asociadas al perfil denunciado.

Se solicita que se evite formular cualquier tipo de notificación al usuario de la cuenta mencionada y/o su Defensa, a los efectos de asegurar el éxito de la investigación.

Asimismo se hace saber que la información requerida ha sido solicitada por la Fiscal interviniente en estas actuaciones, Dra. Daniela Silvina Dupuy, a cargo de la Unidad Especializada en Delitos y Contravenciones Informáticas del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires, en el marco de la investigación registrada bajo el N° MPF 522910.

Se autoriza al Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal el diligenciamiento del presente y la recepción de la información requerida.

Saludo a Ud. muy atentamente.


1.3 Solicitud de información de contenido

Teniendo en cuenta que la empresa Google Inc. se encuentra radicada en los E.E.U.U., la petición deberá ser cursada bajo los términos establecidos en el Ley 24.034, la que aprobó el Tratado de Asistencia Mutua en Asuntos Penales con el Gobierno de Estados Unidos.

1.4 Casos de emergencia

Ante casos de emergencias, fundados en la posibilidad concreta de que una persona se encuentre en riesgo de muerte o sufra daños físicos graves, se podrá requerir información a la firma Microsoft Inc. a través de la casilla **LEALERT@microsoft.com** cumpliendo con idénticos requisitos que los pedidos normales de información y completando el formulario que debajo se adjunta.

Microsoft Corporation, USA

 Select one of these entities

Microsoft Ireland Operations Limited, Ireland

(European Countries only)

Pursuant to Title 18 U.S.C. §2702(b)(8) and §2702(c), Microsoft may disclose relevant data in emergency situations “if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person” requires immediate disclosure of information. If you believe an emergency situation meets the legal standard set forth above, please provide as much information as possible to allow Microsoft to make that determination. We will not respond to requests submitted by non-law enforcement officials. **All fields are required.**

1. Describe the nature of the emergency, providing specifics as to why this is an immediate threat to life

2. Provide the target account(s) and specify the service (Outlook/Hotmail, Xbox, Skype, etc.)

3. What data are you seeking to obtain from the target account(s)? **(be specific)**

4. Government-issued email address (this is where responsive data will be sent)

5. Contact information of LE official making this request (name, agency, phone number - may attach business card)

I attest that the above-mentioned facts are true and accurate to the best of my knowledge. I further attest that this request involves immediate danger of death or serious physical injury and requires disclosure of the requested information without delay.

Printed Name and Signature (e-signature NOT accepted)

Date

Return this form to: LEALERT@microsoft.com



2. Facebook, Instagram y WhatsApp

Facebook, Instagram y WhatsApp responden sus solicitudes a través de un portal por ellos mismos provisto.

De esta manera, como primera medida debemos registrarnos en él. Facebook e Instagram nucléan funcionan bajo el portal que se accede desde la URL www.facebook.com/records y WhatsApp gestiona las peticiones a través de su propio portal, que se accede a través de la URL www.whatsapp.com/records.

Ahora bien, teniendo en cuenta que la interfaz de dichos portales es exactamente igual a la vista del usuario, se realizará toda la explicación tomando como ejemplo el portal de Facebook.

¿Qué tipo de pedidos se puede realizar a la empresa?

- Conservación de datos de la cuenta investigada
- Solicitud de información de registración y logueo
- Solicitud de información de contenido

Ingreso y Registracion

Para comenzar a utilizar la plataforma para agentes de la Ley de la firma Facebook, primero debemos registrarnos.

Para ello, tendremos que ingresar al siguiente link www.facebook.com/records.

Unas vez dentro, nos solicitará que tildemos la opción que reza *“I am an authorized law enforcement agent or government employee investigating an emergency, and this*

is an official request” (Soy un agente de la ley autorizado o un empleado del gobierno que investiga una emergencia, y esta es una solicitud oficial).

facebook

Law Enforcement Online Requests



We are currently experiencing delays in responding to requests. We are working to resolve this as quickly as possible. If this is an emergency matter, or needs special attention, please respond with a detailed explanation and your request will be reviewed immediately.

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

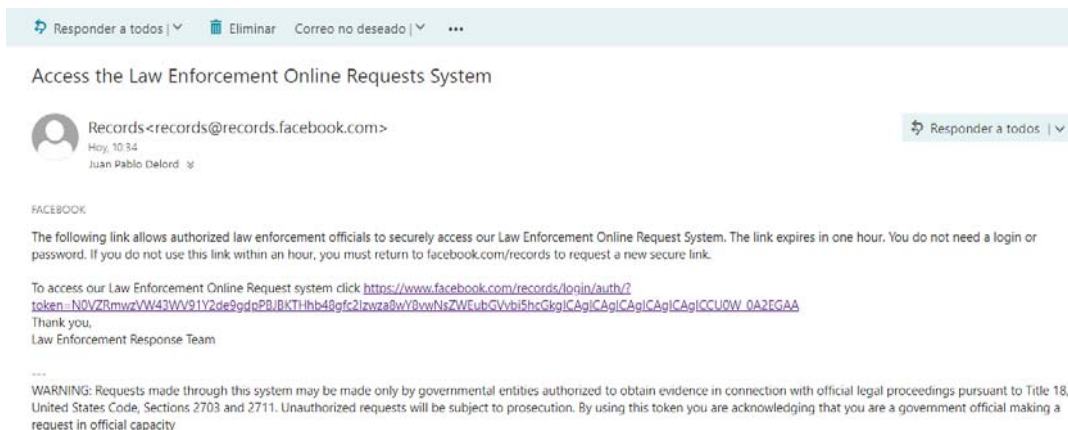
Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.

English (US) Español Português (Brasil) Italiano Français (France) العربية Deutsch 中文(简体) हिन्दी 日本語 +

Hecho ello, nos permitirá clikear “Request Accesess”, y al hacerlo nos solicitará ingresar un correo electrónico gubernamental (.gov.ar ó gob.ar) al cual se enviara al mail ingresado, un link para el ingreso y la registracion.

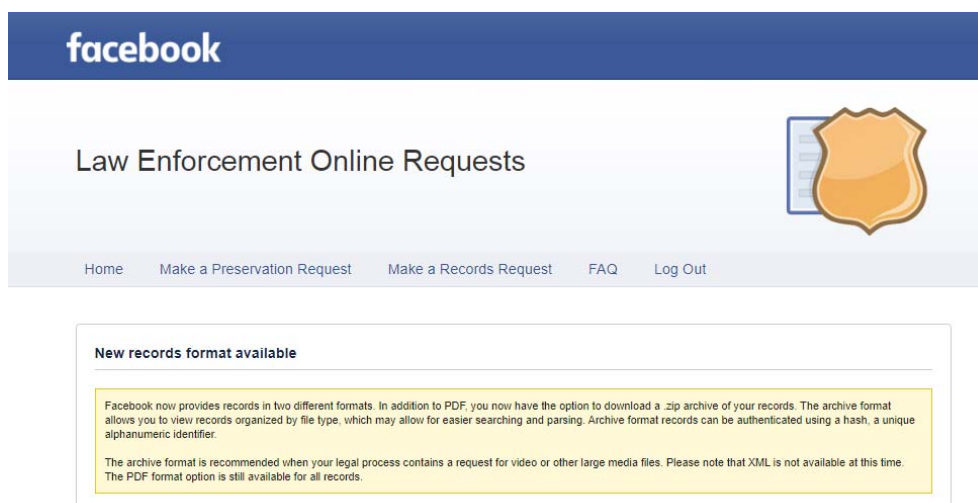
The screenshot shows the Facebook 'Law Enforcement Online Requests' page. A modal dialog box titled 'Request Access' is open, prompting the user to enter an email address. The dialog box contains the following text: 'Email: [input field]', 'Enter your email address to receive a unique link to the Law Enforcement Online Request System. The link will give you access to the system for one hour.', and 'Cancel Submit' buttons. In the background, the page content is visible, including the 'Request Secure Access to the Law Enforcement Online Request System' section, the 'Request Access' button, and the warning text.



A continuación, se deberá ingresar al Link aportado por Facebook y cargar los datos requeridos, para así finalizar el paso de registración.



Una vez logrado el acceso al Portal, el mismo se verá de la siguiente manera:



Se encuentra integrado por cinco solapas “Home”, “Make a Preservation Request”, “Make a Records Request”, “FAQ” y “Log Out”, las cuales detallaremos a continuación.

“HOME”: Por default nos ubicaremos allí cada vez que ingresemos al portal. Aquí podremos observar el estado de todas las intervenciones solicitadas, como pedidos de conservación o de datos. De allí también se descargará la información que Facebook aporte.

“Make a Preservation Request”: Aquí ingresaremos para solicitar las preservaciones de datos de las cuentas.

“Make a Records Request”: Esta opción es para realizar los requerimientos de información de los usuarios.

“FAQ”: Preguntas frecuentes

“Log Out”: Cerrar sesión.

2.1 Conservación

Facebook ofrece la posibilidad de, previo a realizar el requerimiento de información, solicitar la conservación de los datos de cuentas en relación con una investigación penal oficial durante 90 días, la cual se debe hacer a través del sistema de solicitudes por Internet para fuerzas del orden, sin la necesidad de confeccionar un oficio para ello.

Se debe ingresar al portal repitiendo el paso 1 y 2 anteriormente mencionado. Una vez dentro, debemos seleccionar la solapa “*Make a Preservation Request*”.



Allí, nos solicitar información básica de la cuenta a conservar.

- **Internal Case Reference Number**: Número nuestro expediente o caso, a los efectos de poder individualizarlo en la solapa de “Home”.
- **Accounts**: Aquí Debemos indicar si corresponde a un perfil de Facebook o Instagram, y seguidamente nos pedirá que ingresemos una fecha y un texto libre para identificar al usuario. Con respecto al texto libre, tenemos cuatro opciones para escribir (siempre relacionado con el perfil en cuestión”:
 - Dirección de correo electrónico.
 - Número de teléfono (+XXXXXXXXXXXX).
 - Número de identificación de usuario -ID-
http://www.facebook.com/profile.php?id=1000000XXXXXXXX
 - Nombre de usuario (http://www.facebook.com/username)

Ahora bien, en relación a la fecha, es fundamental ingresar el día en que estemos totalmente seguros que ese ID, SUAURIO O URL se corresponda con el perfil investigado.

- **Requesting Records Between**: en este apartado, se deberá consignar el rango de fechas de los accesos registrados que deseamos que Facebook conserve.

2.2 Solicitud De Información de registración y conexión


La petición se hará a través del portal provisto por la propia empresa, debiendo adjuntarse a la petición un oficio en formato .pdf o .jpg que cumpla con los siguientes requisitos:

- Oficio con **fecha actual, firmado por parte del Juez** interviniente en la investigación, solicitando que se informen los siguientes datos: (i). Del Registro de Información Transaccional; (ii). Del Registro de direcciones IP utilizadas tanto para la creación como para el acceso hasta el presente, con indicación de las fechas y horas pertinentes, (iii). Información Registrada del usuario, (iv). Información sobre eventuales cambios de contraseña.
- El oficio deberá contener sello oval, medalla o sello de la dependencia que emite la solicitud.
- Deberá estar encabezado de la siguiente manera:

Facebook e Instagram	WhatsApp
<p style="text-align: center;">“Facebook Inc. 1601, Willow Road, Menlo Park, CA 94025, EEUU”</p>	<p style="text-align: center;">“WhatsApp Inc.; 1601 Willow Road; Menlo Park, California 94025; United States of America”</p>

- Deberá mencionarse el delito investigado, efectuando una descripción o transcripción del mismo, que permita conocer sobre que versa la investigación.

- Si bien el oficio es librado por parte del Juez del caso, podrá ser diligenciado por el propio Juzgado, Fiscalía o fuerza policial interviniente.
- Para mayor ilustración se acompaña debajo un modelo de oficio dirigido a Facebook.

 Poder Judicial de la Ciudad de Buenos Aires
Fuero Penal Contravencional y de Faltas

Juzgado N° 3 – Secretaría Penal Juvenil

Se solicita no dar aviso al usuario de este requerimiento.

Buenos Aires, 13 de octubre de 2017.-

FACEBOOK Inc.
1601 Willow B
Menlo Park,
CA 94025 - U

Tengo el agrado de dirigirme a usted, en mi carácter de Jueza a cargo del Juzgado en lo Penal, Contravencional y de Faltas n° 3, Secretaría Penal Juvenil a cargo de la Dra. María Mercedes Maiorano, sito en Tacuarí n° 138, piso 10, de esta ciudad (tel: 4014-6862), en relación al Sumario n° [REDACTED] causa n° [REDACTED]/17, caratulado: “DE JULIO [REDACTED] É??¿Qué F?óó s/art. 11179:128parr1 Delitos Atinentes a la Pornografía CP (p/ L 2303)”, a fin de solicitarle quiera tener a bien arbitrar los medios necesarios con el objeto informar, respecto del usuario “http://www.facebook.com/[REDACTED]” los datos que a continuación se detallan:

A) del registro de información transaccional;

B) del registro de direcciones de IP utilizadas tanto para la creación como para el acceso hasta el presente, con indicación de las fechas y horas pertinentes;

C) información registrada del usuario;


D) información sobre eventuales cambios de contraseña y;


E) las distintas y/o sucesivas cuentas de correo asociadas al perfil de Facebook denunciado.-

Asimismo, se hacer saber que no deberá darse aviso al usuario mencionado respecto de las medidas ordenadas, ello dada la naturaleza y estado de la investigación que se lleva a cabo en los autos en que me dirijo.-

Finalmente, le hago saber que se autoriza para el diligenciamiento del presente oficio al Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal.-

Saludo a Usted con distinguida consideración.-


[REDACTED]


[REDACTED]
Secretaría Penal Juvenil

Ahora bien, al momento de ingresar nuestra requisitoria en la plataforma, debemos ingresar en la solapa “*Make a Records Request*”.

The image shows a screenshot of the Facebook Law Enforcement Online Requests form. A red box highlights the "Make a Records Request" button. Another red box highlights the form fields, including a warning about account names and vanities.

Make a Records Request

facebook

Law Enforcement Online Requests

Make a Records Request FAQ Log Out

Requester Information

Email: mshlvs@seccales.gob.ar
 Name: Marina Shlvs
 Title: Oficial
 Organization: Unidad Fiscal Especializada en Delitos y Contrainteligencias Informáticas
 Phone Number: 34.911.520.4100
 Location: Buenos Aires, Argentina

Records Request

Please complete all fields below and be sure to attach all relevant documentation. A U.S. search warrant, Mutual Legal Assistance Treaty (MLAT) or letter rogatory is generally required to compel disclosure of user content.
 The Law Enforcement Response Team reviews each request separately and discloses account records solely in accordance with our terms of service and applicable law. Additional information can be found in the Facebook or Instagram Law Enforcement Guidelines.

Please note that all times are recorded in UTC and adjust your request parameters accordingly.

Internal Case Reference Number [?]

Legal Process: Select One

Nature of Case: Select a Legal Process First

Legal Process Signed Date [?]: dd/mm/yyyy

Request Due Date [?]: dd/mm/yyyy

Accounts: Facebook, Instagram

Requesting Records Between [?]: Select

Documentation: Seleccionar archivo | No se eligió archivo

Additional Context [?]

I attest that I am a law enforcement agent or government employee authorized to request account records and all the information I have provided is accurate.

Submit

Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

Aquí nos solicitará los mismos datos que en los pasos de “conservación”, agregando la siguiente información que a continuación se detallará.

- **Legal Process:** Nos dará tres opciones a elegir, “*Court Order/Request (Outside US)*”, “*Emergency*” y “*Regulatory/Electoral*”.

Legal Process **Select One** ▼

Nature of Case **Select One**

Legal Process Signed Date [?]

Request Due Date [?]

Accounts

- Court Order/Request (Outside US)
- Emergency
- Regulatory/Electoral

- **Nature of Case:** al expandir la sección, nos otorgará una larga lista de opciones, entre las que se encuentra “Seguridad Infantil”, “Drogas”, “Sumplantación de Cuenta”, “Extorción Sexual”, entre otras.

Legal Process Court Order/Request (Outside ... ▼

Nature of Case **Select One** ▼

Legal Process Signed Date [?]

Request Due Date [?]

Accounts

Requesting Records Between [?]

Documentation

Additional Context [?]

that I am a law enforcement agent or
tion I have provided is accurate.

0

Spanish Portuguese (Brasil) Italiano Français (France) العربية Deutsch 中文(简体) हिन्दी

- Select One**
- Child Safety (No Immediate Threat Identified)
- Child Safety (Potential Harm)
- Drugs/Narcotics
- Fake/Impersonation Account
- Financial Fraud/Scam
- Firearms/Weapons
- Fugitive
- Gang Activity
- Hacked Account
- Homicide/Murder
- Human Smuggling
- Human Trafficking
- Missing/Kidnapped Person
- Missing/Kidnapped/Runaway Minor
- Physical Assault
- Robbery/Theft
- Sex Crime/Sexual Assault
- Sexual Extortion
- Suicide
- Terrorist Activity
- Threats/Harassment
- Criminal Defamation
- Hate Speech
- Other

- **Legal Process Signed Date:** Aquí debemos ingresar la fecha en la que se confeccionó y que posee el oficio en cuestión.

- **Request Due Date**: En esta opción, indicaremos una “fecha de vencimiento” de la solicitud.
- **Documentation**: para que Facebook le de curso a nuestro requerimiento, se tendrá que adjuntar sin falta un oficio emitido por el juzgado que interviene en el caso y firmado por su titular, junto con documentación relativa al hecho a estudio (Ej.: Denuncia, Decreto de Determinación de los Hechos, impresiones de pantalla de la cuenta investigada, etc.). Debemos tener en cuenta que si lo que adjuntamos no le resulta convincente al operador de la firma extranjera que tramitará nuestra intervención, se nos solicitara más información al respecto.
- **Additional Context**: Aquí nos da la opción de ingresar un texto libre, donde podremos explicar brevemente nuestro hecho manifestando además la necesidad e importancia de nuestra solicitud.



3. PAYPAL

Recibe todas las peticiones a través del portal provisto por la propia firma a través de la URL <https://safetyhub.paypal.com>

Ingreso y Registracion

Para comenzar a utilizar la plataforma para agentes de la Ley de Paypal, primero debemos registrarnos cumpliendo con todos los pasos que se detallan en el documento provisto por la empresa que se adjunta a la presente guía.

¿Qué tipo de pedidos se puede realizar a la empresa?

- Solicitud de información de registración y logueo
- Solicitud de información de contenido

3.1 Conservación de información

La petición se hará vía correo electrónico desde una cuenta gubernamental -.gov.ar o .gob.ar - a través de la cuenta lawenforcement@paypal.com en la que se deberá adjuntar un oficio en formato .pdf o .jpg que cumpla con los siguientes requisitos:

- Estar dirigida a:

Paypal Pte. Ltd.
Global Investigation Team
2211 North First Street, San Jose
CA 95131, USA

- El oficio que se adjunte, deberá estar confeccionado por cualquier funcionario de Fiscalía, Juzgado o fuerza policial interviniente.
- Dicho oficio deberá contener una descripción del tipo de delito investigado y estar firmado por la autoridad que emite la solicitud, el cual puede ser cualquier funcionario judicial y/o policial, como así también se debe detallar la información específica que se requiere sobre la dirección de correo electrónico o en su caso la conservación de datos

3.2 Solicitud de información de registración y logueo y contenido

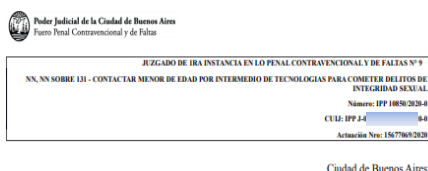
La petición se hará vía a través del portal provisto por la empresa en la URL <https://safetyhub.paypal>. en la que se deberá adjuntar un oficio en formato .pdf o .jpg que cumpla con los siguientes requisitos:

- Oficio con **fecha actual, firmado** por parte del **Juez interviniente** en la investigación, solicitando que se informen los siguientes datos: (i). Del Registro de Información Transaccional; (ii). Del Registro de direcciones IP utilizadas tanto para la creación como para el acceso hasta el presente, con indicación de las fechas y horas pertinentes, (iii). Información Registrada del usuario, (iv). Información sobre eventuales cambios de contraseña.

- El oficio deberá contener sello oval, medalla o sello de la dependencia que emite la solicitud.
- Deberá estar encabezado de la siguiente manera:

Paypal Pte. Ltd.
Global Investigation Team
2211 North First Street, San Jose
CA 95131, USA

- Deberá mencionarse el delito investigado, efectuando una descripción o transcripción del mismo, que permita conocer sobre que versa la investigación. La empresa restringe sus respuestas a casos de gravedad donde se encuentre en riesgo la integridad física de una persona.
- Si bien el oficio es librado por parte del Juez del caso, podrá ser diligenciado por el propio Juzgado, Fiscalía o fuerza policial interviniente a través del portal que ellos proveen.
- A continuación, se exhibe un modelo de oficio.



PayPal Pte. Ltd.
Global Investigations Team,
2211 North First Street, San Jose,
CA 95131, USA

SD

Tengo el agrado de dirigirme a Ud., en el marco de la investigación penal registrada bajo el N° [redacted] caratulada "NN sobre 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL CP (p/ L 2303)", en trámite por ante este Juzgado Penal, Contravencional y de Faltas N° 9 (sito en la calle Beruti 3345, piso 4, de esta ciudad, Tel: 401 [redacted]) a mi cargo, a fin de solicitarle tenga a bien aportar los datos de registración y conexión relativos a la cuenta con nombre "milagros [redacted]roia", cuyo ID de comercio es "X [redacted]/RPPL".

Se hace saber que motiva la presente requisitoria la investigación llevada a cabo por la Unidad Especializada en Delitos y Contravenciones nro. MF [redacted] y que su titular, Dra. Daniela Dupuy encuadró el hecho investigado en los términos del art. 131, del Código Penal que establece: "Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. (Artículo incorporado por art. 1º de la Ley N° 26.904 B.O. 11/12/2013)".

Asimismo, en atención a la medida dispuesta, se solicita no dar aviso al usuario de este requerimiento.

Por último, delego el diligenciamiento del presente oficio a la Unidad Especializada en Delitos y Contravenciones, donde se deberá remitir la totalidad de la información recabada.

Saludo muy atentamente.

Una vez que contamos con el oficio debemos acceder a la plataforma y cargar el pedido de información cumpliendo con los datos que solicita el portal.



Material adicional

A continuación, se detallan sitios de utilidad para avanzar en investigaciones en entornos digitales, así también, se facilitan enlaces que remiten a guías para realizar peticiones a distintas empresas radicadas en el extranjero, donde cada una de ellas, detallan los requisitos y vías a través de las cuales deben ser canalizados los pedidos.

Sitios para determinar que empresas administra cada IP

- <http://www.iplocation.net> o rdap-web.lacnic.net

Listado de prestadoras de servicios de Internet en Argentina

- <http://icannlac.org/PO/isps-ar>

Sitio para realizar conversiones horarias

- <https://www.worldtimebuddy.com/>

Sitios para consultar dominios

- www.whois.net
- <http://www.nic.ar>

Políticas internas de cada empresa extranjera en torno a peticiones jurídicas internacionales y mails o canales de contacto

Google

- <https://support.google.com/transparencyreport/answer/9713961?hl=en>
- Portal Google <https://lers.google.com/>

Microsoft

- <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>
- Portal Microsoft <https://leportal.microsoft.com/home>

Facebook

- <https://www.facebook.com/safety/groups/law/guidelines/>
- Portal Facebook e Instagram <https://www.facebook.com/records/login/>

WhatsApp

- <https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities>
- Portal WhatsApp <https://www.whatsapp.com/records/login/>

Twitter

- <https://help.twitter.com/forms/lawenforcement>

TikTok

- <https://www.tiktok.com/legal/law-enforcement>

Netflix

- info@mailier.netflix.com

Kik

- lawenforcement@kik.com

Yahoo Argentina

- Se diligencia oficio en papel ante las oficinas que la empresa posee en Av. del Libertador 498, piso 23, CABA

Tagged

- LawEnforcement@themeetgroup.com.

Rapipago

- Rapipago (GIRE S.A)
- Av. Caseros 3572 CABA
- LLEGALES@gire.com.ar
- <mailto:infolegales@rapipago.com.ar>
- teléfono: 4324-1500 interno: 20937.

Tumblr

- https://www.tumblr.com/docs/en/law_enforcement

Mercado Libre

- notificaciones@mercadolibre.com

Links Actualizados (Junio 2026)

ICANN - Registration data lookup tool

<https://lookup.icann.org/en>

MiLACNIC Query

(Geolocalizar IPS y dominios de páginas web)

<https://query.milacnic.lacnic.net/home>