2021

# Guía de Obtención de Evidencia Digital de Proveedores en el Extranjero

REMPM | Reunión Especializada de Ministerios Públicos del Mercosur

MERCOSUR

REUNIÓN ESPECIALIZADA DE **MINISTERIOS PÚBLICOS** DEL MERCOSUR

MERCOSUL

2021

# Guía de Obtención de Evidencia Digital de Proveedores en el Extranjero

REMPM | Reunión Especializada de Ministerios Públicos del Mercosur

**Guía de Obtención de Evidencia Digital de Proveedores en el Extranjero.**

REMPM | Reunión Especializada de Ministerios Públicos del Mercosur

---

Edición: septiembre 2021

## Índice

INTRODUCCIÓN ..... 7

I. GLOSARIO ..... 8

II. CLASES DE INFORMACIÓN Y FORMAS DE OBTENERLA ..... 10

III. PRESERVACIÓN DE INFORMACIÓN ..... 14

IV. CÓMO SOLICITAR UNA PRESERVACIÓN O INFORMACIÓN BÁSICA DEL SUSCRIPTOR ..... 16

V. REQUERIMIENTOS DE ASISTENCIA LEGAL MUTUA (MLAT) O EXHORTO ..... 18

VI. CASOS DE EMERGENCIA ..... 20

VII. FUENTES ABIERTAS ..... 21

VIII. ANEXOS ..... 23

## INTRODUCCIÓN

El objetivo de este documento es brindar a las y los investigadores una herramienta de consulta, con carácter operativo, que sirva de Guía en caso de que necesiten obtener información electrónica almacenada en el extranjero.

La experiencia indica que la mayoría de las empresas a las que se suele pedir información en el marco de investigaciones penales se encuentran radicadas en los Estados Unidos de América (EUA) o en la Unión Europea (EU), por lo que haremos especial foco en las regulaciones que nos permiten solicitar información a compañías radicadas dichas jurisdicciones.

Las recomendaciones sistematizadas en este material fueron elaboradas conjuntamente por Representantes de los Ministerios Públicos Fiscales de Latinoamérica, sobre la base de documentos oficiales y la experiencia adquirida a lo largo de años de trabajo.

Destacamos que algunos países que han contribuido a la elaboración de la presente Guía son Estados partes u observadores del Convenio sobre Ciberdelito del Consejo de Europa (ETS N° 185), también conocida como Convención de Budapest[1].

Por último, y sin perjuicio de que la intención de este documento es perdurar en el tiempo, detallaremos sobre el final los requisitos de aquellas empresas a las que más se suelen pedir medidas. Destacamos que los requisitos pueden eventualmente variar, y que siempre resultará conveniente al investigador acudir a las propias plataformas o solicitar la asistencia de la Unidad Especializada de su jurisdicción.

1. https://www.coe.int/en/web/cybercrime/parties-observers

## I. GLOSARIO

A continuación, se entregan definiciones de una serie de conceptos que son usados a lo largo de esta guía. Estos conceptos pueden o no encontrarse definidos en las legislaciones nacionales vigentes. En su mayoría corresponde a aquellos que se encuentran en el Convenio de Budapest.

**Evidencia digital:** Toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio. Incluye tanto aquella contenida en dispositivos electrónicos como la transmitida electrónicamente a través de redes de comunicación.

**Sistema informático:** Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. En otras palabras, se trata de un sistema que permite almacenar y procesar información en forma de dato informático.

**Dato informático:** Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

**Proveedor de servicio:** Toda entidad pública o privada que brinde a los usuarios de sus servicios la posibilidad de comunicarse entre sí por medio de un sistema informático, como también, cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.

**Información de suscriptor:** Consiste en toda información, en forma de datos informáticos o en cualquier otro formato, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, el periodo del servicio, dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, correo electrónico, información sobre facturación y medio de pago, o información relacionada con el abonado adicional que se encuentre en manos de dicho proveedor.

**Dirección IP (Internet Protocol):** El Protocolo de Internet o IP (*Internet Protocol*) es el conjunto de reglas de comunicación, que permite que las diferentes redes funcionen unas con otras. El Protocolo de Internet especifica que cada dispositivo de la red global necesita un identificador número único, una dirección que permita encontrarlo, lo que se conoce como una dirección IP. Hoy en día, en internet se utilizan dos versiones de IP. La versión antigua, que se utiliza desde 1983 y sigue siendo la más usada a nivel mundial, llamada IPv4. Y la versión actual, cuyo uso en la red está aumentando rápidamente: IPv6.

**Dirección IP estática:** Dirección IP asignada por un proveedor de servicios en internet a un abonado

de forma estable durante la duración de la contratación de servicios. Por el hecho de ser asignada de manera estable a un abonado, el proveedor de servicios puede buscar la dirección IP en una base de datos para poder vincularla a quién hace uso de ella.

**Dirección IP dinámica:** Dirección IP asignada por un proveedor de servicios de acceso a Internet a un usuario de manera temporal, pudiendo ser otorgada luego a otro.

**Log:** Registro cronológico de actividades en un sistema informático (por ejemplo, en un programa, una aplicación o un servidor). Así, los proveedores de servicio tienen un listado de conexiones que sus abonados realizan a sus servicios.

**IMEI (International Mobile Equipment Identity):** Corresponde a una serie de números inalterables que se incorporan obligatoriamente por el fabricante en los dispositivos móviles y que permiten identificar dicho dispositivo respecto de cualquier otro equipo físico, con independencia del abonado que haga uso de dicho terminal.

**IMSI:** Código que se inserta en la tarjeta SIM (*Suscriber Identity Module*) posibilitando la identificación internacional de quién ha contratado una línea de servicios móviles.

## II. CLASES DE INFORMACIÓN Y FORMAS DE OBTENERLA

Las pautas y recomendaciones comprendidas en esta Guía se centran exclusivamente en la preservación y obtención de evidencia electrónica almacenada por los proveedores de servicios, y no en la obtención en tiempo real de comunicaciones.

En este sentido, concentramos el análisis en la información almacenada, relacionada con cuentas de correo electrónico y redes sociales (datos del usuario, historial de conexiones, contenido de los mensajes, etc.) u otros servicios de internet (como registro de nombres de dominio o alojamiento de sitios web), que es la que usualmente se solicita.

Para comprender las distinciones entre las diversas clases de información resulta útil analizar tanto la legislación de los Estados Unidos de América (EUA) como las disposiciones del Convenio de Budapest, ambos instrumentos clasifican los registros en función de la mayor o menor invasión a la privacidad del usuario. En otros términos, cuanto mayor sea el grado de intrusión requerido, más altos serán los estándares que deberán satisfacerse para obtener la información.

De esta manera tenemos tres grupos de información: básica, transaccional y de contenido.

a. Información básica del suscriptor, que incluye usualmente:

- Datos declarados por el titular de la cuenta (nombre, país, dirección, teléfonos, edad, género, etcétera)
- Dirección de correo electrónico asociada (usada generalmente para verificar/recuperar la cuenta).
- Número de teléfono celular asociado (usado generalmente para verificar/recuperar la cuenta).
- Número de tarjeta de crédito asociada (que se brinda para hacer compras en la plataforma).
- Dirección IP desde la que se creó la cuenta.
- Detalle de los últimos accesos a la cuenta (con fecha, hora, huso horario y dirección IP).
- Información sobre servicios a los que se ha suscripto el titular de la cuenta2.

2. En el caso de una cuenta Gmail, por ejemplo, indicará qué otros productos de Google LLC. se encuentran asociados a esa cuenta (tales como: YouTube, Google+, etcétera).

Cabe señalar que muchos de estos datos son aportados por el usuario al momento de registrarse en una aplicación o plataforma y son meramente declarativos. Muchas empresas indican en sus informes si los datos han sido verificados (*verified*). Esto suele suceder cuando la empresa envía un correo electrónico o un código por mensaje de texto al usuario para que confirme/finalice su suscripción, por ejemplo.

La obtención de esta información está sujeta al estándar de citación: sólo hay que demostrar que la misma es relevante y está relacionada con el caso.

Usualmente esa información es entregada por las empresas a autoridades judiciales extranjeras **sin necesidad de emitir una solicitud de asistencia jurídica (MLAT).** En la mayoría de los casos, bastará enviar un **oficio firmado, usualmente por el juez** por algunos de los canales habilitados al efecto[3].

Al respecto, la Convención de Budapest establece en su artículo 18.1.b. que se habilita a las autoridades competentes para ordenar que: "*un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios"*.

Las empresas radicadas en EUA encuentran fundamento/autorización legal para brindarnos esta información en el Título 18, Sección 2703 (c) de la Ley Federal de Comunicaciones almacenadas (*Federal Stored Communications Act*) del Código de los Estados Unidos. Resulta importante destacar que esta no es una obligación legal, por tal motivo, si la empresa conforme sus políticas (localización o actividad de la cuenta, tipo de caso investigado en nuestro país, etc.) decide no compartir la información con las autoridades requirentes, será necesario enviar una solicitud de asistencia jurídica para que un juez de Estados Unidos emita una orden en ese sentido.

b. Información transaccional o Tráfico de IP corresponde a cualquier dato informático relativo a una comunicación que se haya transmitido por un medio de un sistema informático, que haya sido generado por un sistema informático como elemento de la cadena de comunicación y que indique el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o tipo de servicio subyacente.

En estos casos, el estándar impone mayores exigencias. Se van a requerir detalles específicos acerca de cómo los registros son relevantes para la investigación. La experiencia indica que esta información sólo será entregada si media una orden de un juez local, para lo cual será necesario enviar una solicitud de asistencia jurídica internacional.

c. Información de contenido, corresponde a todos aquellos datos informáticos almacenados en un sistema informático, que incluyen usualmente:

3. Muchas empresas proveedoras de servicios de internet han establecido portales o casillas de correo electrónico para que las fuerzas de seguridad o autoridades judiciales puedan cursar sus pedidos.

- Contenido (texto y adjuntos) de los correos electrónicos que permanezcan en las carpetas de la cuenta (enviados, recibidos, borrador, papelera, etcétera).

- Contenido (texto y adjuntos) de los mensajes intercambiados en plataformas de redes sociales[4].

- Contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general[5].

- Historial de localización asociado a una cuenta.

- Fotos y otros documentos almacenados por el usuario en espacios de alojamiento en la nube asociados a una cuenta.

La obtención de esta información está sujeta al estándar más alto: el de orden de allanamiento, basado en una causa probable actual. También será necesario, en este caso, utilizar una **solicitud de asistencia jurídica internacional** (exhorto internacional).

4. Debe tenerse en cuenta que, entre las diferentes plataformas que admiten el envío de mensajes entre usuarios, se advierte una tendencia hacia la encriptación de su contenido mediante un sistema que, en ciertos casos, impide que los propios proveedores del servicio puedan acceder a la información.

5. Por ejemplo, publicaciones en cuentas privadas de Twitter o biografías de grupos cerrados de Facebook.

## PARA TENER EN CUENTA:

Nada obsta a que los diversos tipos de información sean pedidos en paralelo (por ejemplo, pedir la información de suscriptor por oficio y la de contenido por exhorto).

En ciertos casos, no importará donde estén almacenados en concreto los datos buscados. En los Estados Unidos de Norteamérica, en función de la Ley Federal de Aclaración del Uso Legítimo de Datos en el Extranjero (*Clarifying Lawful Overseas Use of Data Act or CLOUD Act*), promulgada en 2018, que reformó la *Federal Stored Communications Act* citada anteriormente, se permite que las fuerzas del orden público federales obliguen a las empresas de tecnología con sede en Estados Unidos, mediante una orden judicial o citación, a proporcionar los datos requeridos almacenados en sus servidores, independientemente de si los datos se resguardan en suelo estadounidense o extranjero.

Los investigadores deben tener en cuenta que la empresa puede llegar a notificar al usuario de la existencia de un pedido de preservación y/o de entrega de datos (cualquiera sea el tipo) y que eso puede frustrar la investigación. Se recomienda analizar la política de la empresa en ese sentido y, de ser posible, siempre solicitar a las empresas que eviten notificar al titular de la cuenta sobre el pedido de preservación y/o información. Es posible que en estos casos las empresas soliciten que la orden de no revelar la existencia del pedido sea emitida por un juez local y que se pidan razones concretas para hacerlo.

## III. PRESERVACIÓN DE INFORMACIÓN

La información que almacenan los proveedores de servicios puede ser eliminada. Ello puede suceder por acción del usuario, que puede borrar información puntual (por ejemplo fotos, publicaciones, mensajes) o eliminar definitivamente la cuenta, o por el transcurso del tiempo, en tanto razones económicas o de otra naturaleza pueden llevar a que los proveedores decidan almacenar los datos por un periodo limitado (por ejemplo, los *logs* de acceso a las cuentas). Asimismo, las empresas pueden verse obligadas a borrar información por alguna disposición que así se los indique.

**Por ello, teniendo presente la volatilidad de la evidencia digital, se recomienda siempre solicitar la preservación de los datos en cuanto se advierta que podrán ser de interés para la investigación. De acuerdo a nuestra experiencia, algunos datos pueden dejar de estar disponibles en cuestión de minutos, he allí la importancia de realizar la preservación lo más pronto posible.**

La preservación permite mantener a disposición de la autoridad judicial los registros de la cuenta en el momento de materializar la operación, de forma tal que estén disponibles frente a un eventual pedido que se canalice antes del vencimiento de la medida.

Debe tenerse en cuenta que tal proceder no implica el bloqueo de la cuenta sino sólo el resguardo de la información almacenada en la cuenta al momento de realizar la medida. El mejor ejemplo para graficar el procedimiento es el de la fotografía: es como tomar una foto de la cuenta en un momento dado.

Entendemos que la medida resultará admisible, a nivel local, en función del principio de libertad probatoria. Para aquellos países que son parte de la Convención de Cibercrimen, su validez encuentra sustento también en el artículo 16, en tanto prevé que las Partes adoptarán las medidas legislativas o de otro tipo (...) para: 1) *ordenar o imponer de otro modo la conservación inmediata de datos electrónico especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdidas o de modificación*.

En lo que respecta a la normativa aplicable a los proveedores estadounidenses, el Título 18, Sección 2703 (f) del Código de los Estados Unidos, estipula que las empresas podrán preservar información por un **plazo de noventa días,** renovable por un lapso similar[6].

Usualmente, cuando se hace la preservación se brinda un número de referencia que recomendamos sea colocado en el pedido de obtención de esa información.

6. Sin perjuicio de ello, hay empresas que preservan información por más tiempo, como Google (1 año) o Microsoft (180 días).

**Concretar la medida no genera una obligación posterior de solicitar los datos resguardados, pero asegura que éstos estén disponibles si se los pide, cualquiera sea la vía escogida (oficio o exhorto) y/o el tipo de información buscada (básica, transaccional o de contenido). Si posteriormente se concluye que los datos preservados no resultan útiles a la investigación, bastará con dejar vencer la medida o solicitar que se deje sin efecto.**

**Si no se hizo con anterioridad, siempre es conveniente preservar los datos antes de solicitar su entrega mediante una solicitud de asistencia.**

## IV. CÓMO SOLICITAR UNA PRESERVACIÓN O INFORMACIÓN BÁSICA DEL SUSCRIPTOR

Solicitar una preservación o información básica del suscriptor suele ser un procedimiento muy sencillo y rápido. La mayoría de los prestadores de servicios importantes cuentan hoy con un portal para las fuerzas de seguridad o un correo electrónico al que contactarse para concretar este tipo de medidas.

Aconsejamos siempre revisar los términos y condiciones de las empresas a las que se les cursará la solicitud. En especial, los aspectos de privacidad (donde indican qué información guardan, por cuánto tiempo y cómo la comparten) y las directrices para las fuerzas de la ley (en las que suele detallarse el procedimiento para cursar los requerimientos).

Sin embargo, dependiendo del proveedor y de la jurisdicción en la que se encuentre localizado, es posible que no se vea dispuesto ni obligado a cumplir con los requerimientos cursados, en forma directa, por autoridades judiciales radicadas en el extranjero.

### Mecanismos alternativos de preservación u obtención de información

Cuando no sea posible contactar a la empresa de la que se trate para preservar registros u obtener información, dependiendo del territorio en el que se encuentre la empresa o la información que se pretende resguardar u obtener, es posible realizar ciertos requerimientos a través de los siguientes puntos de contacto:

#### 1. Red 24/7 de la Convención de Budapest

El artículo 35 de la Convención sobre Ciberdelito establece que: 1. *Las Partes designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:*

- aportación de consejos técnicos;
- conservación de datos según lo dispuesto en los artículos 29 (“Conservación rápida de datos informáticos almacenados”) y 30 (“Revelación rápida de datos conservados”); y
- recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

## 2. Asociación Iberoamericana de Ministerios Públicos (AIAMP)

La cooperación interinstitucional entre Ministerios Públicos ofrece un intercambio de información para las investigaciones penales ágil y seguro, sobre una base de conocimiento mutuo y confianza entre sus puntos de contacto.

La cooperación directa o interinstitucional se ha consolidado como una herramienta fundamental de la cooperación internacional, ya sea para requerir información o documentación de manera autónoma o para preparar un requerimiento de asistencia jurídica formal.

La suscripción del **Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos miembros de la Asociación Iberoamericana de Ministerios Públicos** (AIAMP), plasma el compromiso de cooperar de manera directa en el marco de investigaciones judiciales, al establecer en su cláusula tercera, **que los Ministerios Públicos de los países que pertenecen a la red**, en su carácter de autoridades competentes, deben cooperar entre sí intercambiando información de manera directa en el marco de investigaciones.

## 3. Red 24/7 de crímenes de alta tecnología del G7

La red 24/7 de crímenes de alta tecnología del G7[7] **(G7 24/7 *Network of High Tech Crime*)**. La red está pensada para las investigaciones que involucran evidencia electrónica y que requieren asistencia urgente de miembros de fuerzas de seguridad o de autoridades judiciales extranjeras, para preservar datos alojados en otros países, en particular, aquellos que no son miembros de la Convención (por ejemplo, Rusia).

## 4. OCN Interpol.

En algunos casos podrá solicitarse la asistencia de la Oficina Central Nacional (OCN) de Interpol para que le requiera a su par en el mundo, según corresponda, asistencia para contactar a una empresa, ya sea sólo para conocer los requisitos necesarios para preservar o requerir información; o ya sea para concretar algunas de estas medidas[8].

**Tal como se ha mencionado, las vías para remitir un pedido de preservación o de entrega voluntaria de información de suscriptor son diversas, recomendamos siempre utilizar la vía más directa posible que generalmente suele ser la solicitud a la empresa. Cuando ello no sea posible, la elección de la red de cooperación para transmitir el pedido dependerá de si la empresa requerida está o no dentro de los países miembros de cada una de ellas.**

---

7. El protocolo de la red prevé que los agentes policiales o judiciales que necesiten asistencia de otro país miembro se comuniquen con su punto de contacto nacional para que éste, a su vez, curse el pedido -de corresponder- a su contraparte en el país requerido. Sus miembros están comprometidos a realizar su mejor esfuerzo para lograr que la asistencia se brinde lo más rápidamente posible, pero se tiene presente que ello depende del marco legal y capacidad técnica de cada uno de los países.

8. La experiencia dicta que se ha podido obtener por esta vía información básica del suscriptor y operaciones con criptomonedas de LocalBitcoins, mediante el libramiento de un oficio librado por el juez del caso y diligenciado por medio de la OCN de Interpol a su par en Helsinky. Cabe aclarar que la empresa entrega datos de contenido sólo vía exhorto.

## V. REQUERIMIENTOS DE ASISTENCIA LEGAL MUTUA (MLAT) O EXHORTO

Cada país fundará el requerimiento de asistencia legal mutua, en primer lugar, en base a los Tratados vigentes sobre asistencia jurídica mutua en materia penal (MLAT, por sus siglas en inglés).

Si no se contara con un instrumento bilateral de estas características con el país del que se intenta obtener información, se podrá fundar el pedido en otros instrumentos internacionales que hayan ratificado ambos países. El más relevante será el Convenio sobre la Ciberdelincuencia o Convención de Budapest–ley 27411-, que tiene la ventaja de estar previsto específicamente para este tipo de situaciones. También podrán citarse la Convención Interamericana sobre Asistencia Mutua en Materia Penal, y dependiendo del caso, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional que tiene normas sobre vigilancia electrónica y sobre operaciones encubiertas para un limitado número de delitos.

Tal como lo adelantamos ya, la mayoría de los proveedores de servicio a los que solemos requerir información se encuentran radicados en los Estados Unidos de América, por lo que resulta importante destacar algunas características propias de dicha legislación.

En primer lugar, es necesario tener presente que la extensión de la protección al derecho de libertad de expresión en dicho país, deja fuera algunas conductas tipificadas en las legislaciones Latinoamericanas, como ser injurias, calumnias, algunos casos de amenazas o de usurpación de identidad. Atento a ello, resultará de interés acompañar documentación que acredite la entidad del hecho investigado. En los casos de amenazas, por ejemplo, será conveniente adjuntar capturas de pantalla a los requerimientos.

En segundo lugar, el estándar para que un juez autorice la divulgación de datos de tráfico y contenido es de “relevancia material” y “causa probable”. El hecho de tener autorización judicial local para solicitar la información ayuda, pero en ningún caso nos releva de la obligación de configurar el estándar de causa probable. El Fiscal en EE.UU tiene que hacer de todas maneras una solicitud al juez competente para poder obtener los datos informáticos que se solicitan. Atendido lo anterior, cabe resaltar la importancia de la preservación previa de los datos, puesto que puede haber cierta demora en reunir los antecedentes que requiera EE.UU para ejecutar nuestra solicitud.

En términos generales, para la confección de un requerimiento de asistencia legal mutua aconsejamos acompañar la siguiente información:

**- Relación cronológica de los hechos y del desarrollo de la investigación.** Se sugiere una redacción como una minuta para juicio abreviado. Debe iniciarse con fecha y contenido de la denuncia, señalar las diligencias que se fueron desarrollando y sus resultados. No se pueden usar frases genéricas como “la investigación determinó” o “se tiene conocimiento que”, cada hecho que afirmamos debe justificarse con un medio de prueba.

**- Causa probable:** se refiere a los antecedentes probatorios que permitan, por un lado, dar verosimilitud a la existencia del hecho delictivo así como a la participación, y, por el otro lado, que permitan explicar por qué las diligencias que se piden son importantes y necesarias para la investigación.

- Los antecedentes de la investigación tienen que indicar que efectivamente vamos a encontrar información relevante para nuestra investigación en la cuenta o correo que estamos consultando. A mayor abundamiento, necesitamos probar que el sospechoso o victima usaba ese medio de comunicación. Por ejemplo, si tengo una víctima de homicidio y quiero saber con quién se contactó por Facebook ese día, tengo que explicar en el requerimiento la evidencia que tengo que la víctima usaba ese medio de comunicación, el hecho de que haya tenido una cuenta de Facebook no es suficiente. En estos casos generalmente se han usado declaraciones de testigos.

**- Teoría del caso del fiscal.** Será necesario dar a conocer las líneas de investigación, lo cual ayuda a las autoridades requeridas a preparar de mejor manera el caso ante el juez y explicar la necesidad de los datos que estamos solicitando. En esta parte también se puede argüir que luego de un número de diligencias de investigación y líneas investigativas los datos que se solicitan corresponden al único antecedente que eventualmente podrían ayudarnos a esclarecer los hechos.

## VI. CASOS DE EMERGENCIA

Más allá del pedido de información (básica, transaccional o de contenido) y de la preservación, en algunos casos las empresas pueden **entregar voluntariamente** información (de suscriptor, de contenido o ambas) **sin necesidad de emitir una solicitud de asistencia jurídica internacional**. El procedimiento se denomina *Emergency Disclosure Request* (EDR).

A esos efectos, debe demostrarse que existe una emergencia que involucra riesgo inmediato de muerte o de seria afectación a la integridad física de una persona, y que esta situación genera que se entregue la información sin demora.

En estos casos el pedido puede realizarse en forma **directa** a las empresas, las cuales evaluarán si el supuesto planteado amerita apartarse de las reglas generales, para lo cual usualmente solicitan información específica al requirente.

Si el pedido es rechazado por la empresa, puede intentar obtenerse la información por los carriles formales.

## VII. FUENTES ABIERTAS

Todo lo señalado precedentemente en esta Guía guarda relación con información que debemos solicitar a los proveedores de servicios. En otras palabras, dicha información se encuentra resguardada por alguna medida de seguridad, como por ejemplo una contraseña, y por lo tanto no es de acceso público.

Por contrapartida, existe una gran cantidad de información que si se encuentra en fuentes abiertas, esto es, cualquier contenido que podemos ver o acceder fácilmente porque está a disposición pública.

El contenido que se encuentra en fuentes abiertas no es necesario pedirlo a los proveedores de servicio, como por ejemplo un perfil de Facebook que es público y al cual podemos acceder porque el usuario de dicho perfil permite que cualquier persona pueda ver la información que comparte, sin agregar barreras de seguridad como podrían ser las solicitudes de amistad.

Varios países cuentan con asentada jurisprudencia en la que se señala que el usuario que ha dejado como pública su información en Internet, ha perdido toda expectativa razonable de privacidad sobre dicha información.

Por lo tanto, cuando en una investigación podamos obtener información de fuentes abiertas no será necesario usar los procesos explicados para solicitar dicho contenido a proveedores de servicios, siendo posible adquirirla directamente de su fuente abierta.

# Anexos

I. Facebook Inc.

II. Google

III. Microsoft Corporation

IV. Tik Tok

V. Twitter Inc.

VI. Whatsapp LLC.

VII. Yahoo! - AOL (Verizon Media)

VIII. Uber

IX. Netflix B.V.

X. PayPal

XI. Otros

# I. Facebook Inc.

# I. FACEBOOK INC.

En primer lugar, recordamos que Facebook Inc. es la propietaria de las redes sociales Facebook e Instagram, motivo por el cual los pedidos que se deseen hacer en relación a cuentas, páginas, publicaciones, etc. de dichas plataformas deberán dirigirse a esa empresa.

## DESCARGA DE INFORMACIÓN.

Adelantamos que la empresa no suele revelar información de la cuenta de la víctima y/o damnificado si entiende que es posible que la persona pueda acceder a los datos por su cuenta.

Por ello, de tener la posibilidad de obtener la información directamente del titular de la cuenta, sugerimos que se le pida que descargue la información buscada.

**Para descargar información de una cuenta de Facebook:**
**https://www.facebook.com/help/212802592074644**

**Para descargar información de una cuenta de Instagram:**
**https://www.facebook.com/help/instagram/181231772500920**

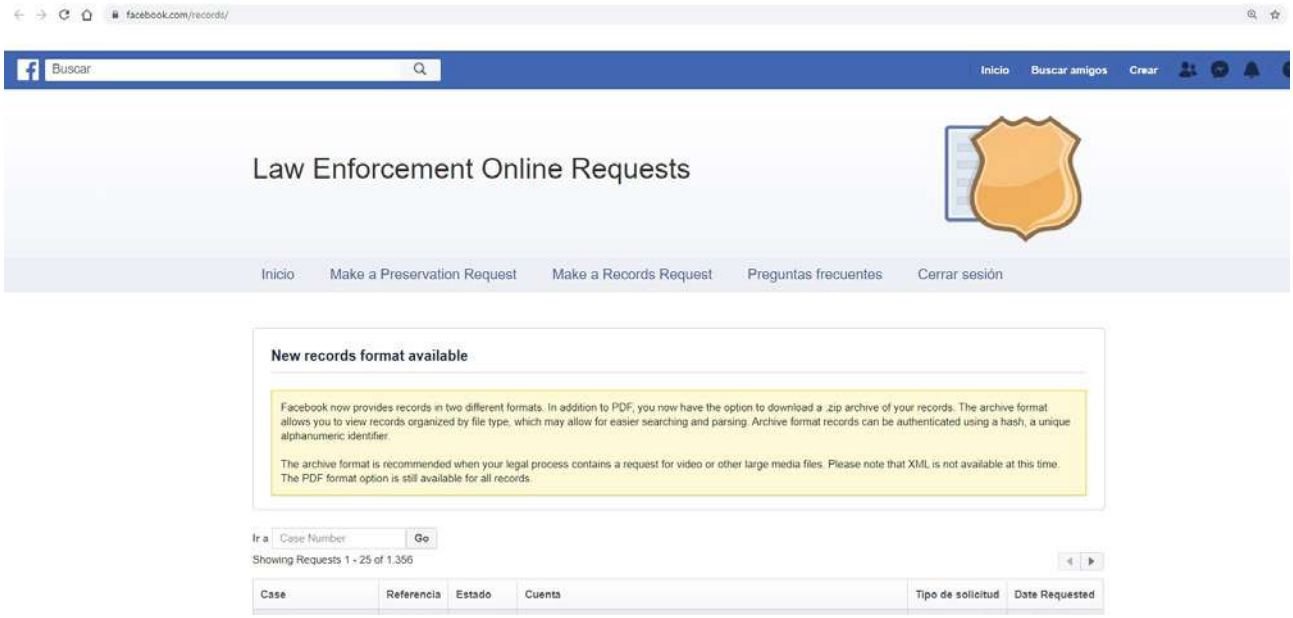
Al momento de solicitar la descarga de la información, aconsejamos que delimiten el pedido a aquellos datos que realmente son útiles para la investigación. Por ejemplo, si lo que se buscan son las conexiones IP de una cuenta en un caso de acceso ilegítimo, puede que las fotografías, mensajes, etc. no sean de interés. Ello, con el propósito de reguardar la privacidad de quien entrega la información.

Recibidos los archivos, recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. Aconsejamos siempre dejar constancia de todo ese procedimiento.

## DILIGENCIAMIENTO DE PEDIDOS.

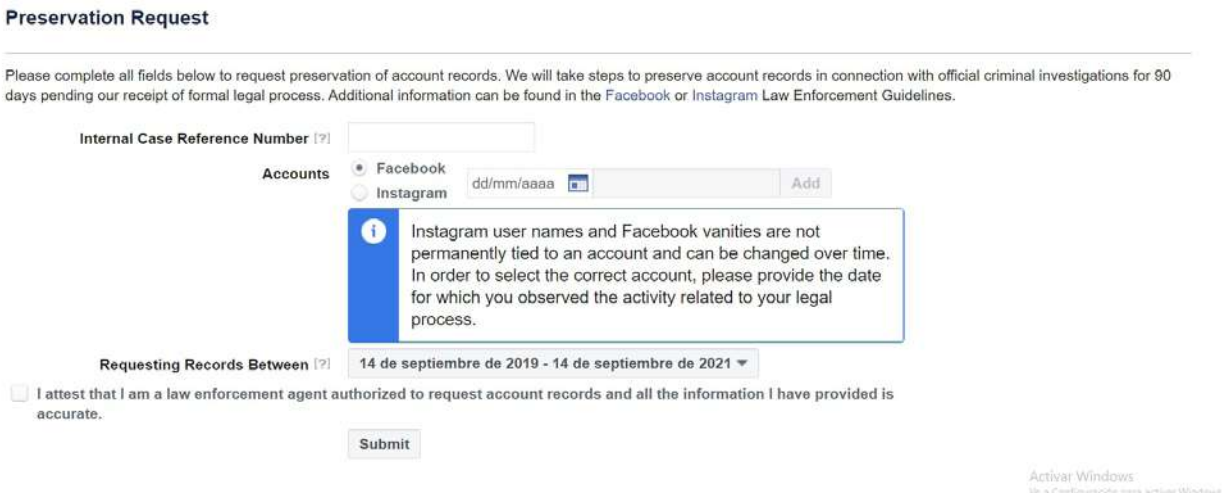
Los pedidos se canalizan exclusivamente a través del portal *Law Enforcement On Line Requests (LEORS)*, al que puede accederse a través del siguiente URL:

**https://www.facebook.com/records**




El portal exige registrarse la primera vez que se ingresa, luego de lo cual sólo tendrá que ingresarse el correo oficial registrado para recibir el enlace al portal, cuya vigencia es de una hora.

A través de dicha plataforma se pueden cursar pedidos de **preservación** llenando el formulario en línea sin acompañar documentos.

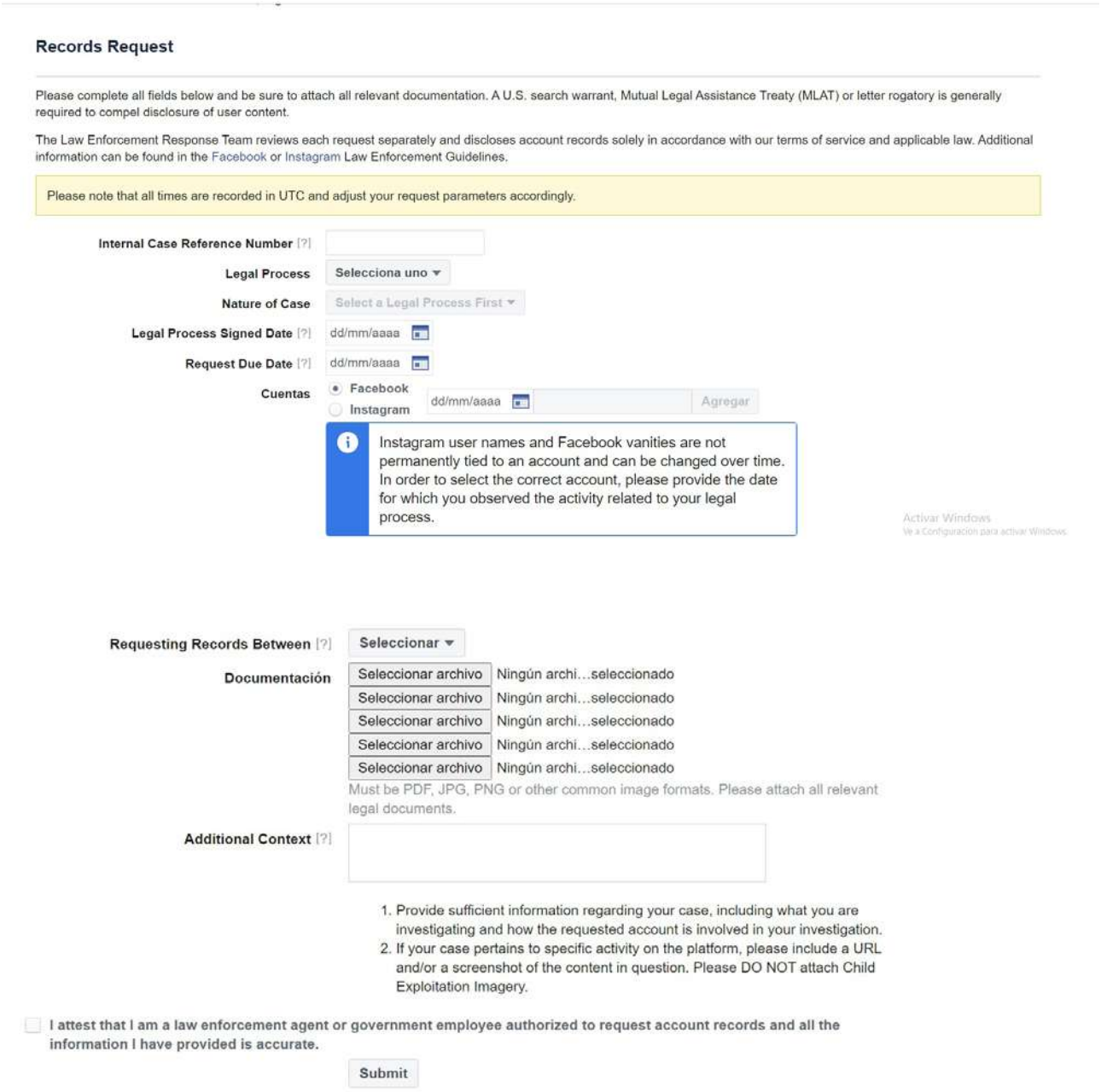



Al cargar una preservación, por defecto el sistema resguarda los registros de los últimos dos años. Si es necesario, puede elegirse un período de tiempo distinto (mayor o menor).

Al enviar el pedido de preservación recibirá un email de confirmación con el número de caso y podrá verificar a través del portal la fecha de vencimiento.

Facebook preserva registros por 90 días, aunque el portal admite extender las preservaciones más de una vez. Bastará simplemente con seleccionar el caso, la cuenta de interés y hacer click en el botón de extender.

Para los pedidos de **entrega voluntaria de información de suscriptor** deben completarse una serie de campos adicionales como el tipo de caso, la fecha de la orden judicial, el período de tiempo de los registros solicitados y debe acompañarse la solicitud en formato .pdf, que se detalla más abajo.



En cualquier caso, sugerimos limitar el pedido a este tipo de información, por cuanto cualquier exceso en el mismo puede motivar un rechazo in *limine*.

En los casos de **revelación de contenido de emergencia** debe llenarse un formulario con preguntas relativas al tipo de caso, la naturaleza de la emergencia, la información deseada, etc. y acompañarse los documentos que permitan respaldar las afirmaciones (capturas de pantalla, fotografías, etc.). El formulario puede ser completado en castellano o en inglés.

Al enviar un pedido de revelación de contenido de emergencia o de entrega voluntaria de información de suscriptor recibirá un email de confirmación de la recepción del pedido y, cuando la información sea procesada, recibirá otro haciéndoselo saber. A través del portal podrá descargar la información entregada en un archivo comprimido y en un documento en formato .pdf.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. En general, el portal informa el valor *hash* en formato SHA 256 del documento comprimido, no del .pdf. Aconsejamos siempre dejar constancia de todo ese procedimiento.

De acuerdo a nuestra experiencia, si el portal no admite la medida por no encontrar registros en sus servidores del identificador seleccionado, ello puede deberse a que el usuario haya borrado su cuenta y consecuentemente la empresa la haya eliminado de sus registros, o que por inacción del usuario, Facebook haya adoptado dicho temperamento. Es decir, si el identificador seleccionado no puede insertarse en el campo correspondiente, la empresa no admitirá la medida solicitada.

## FORMALIDADES DE LOS PEDIDOS.

Les detallamos los requisitos bajo los cuales la empresa accede a entregar información de suscriptor a autoridades de aplicación de la ley ubicadas fuera de los Estados Unidos.

Los pedidos pueden hacerse en castellano, recomendamos utilizar un lenguaje sencillo.

El pedido debe:

- Estar dirigido a **Facebook Inc., 1601 Willow Rd., Menlo Park, CA 94025, California, United States,**
- Indicar número de expediente
- Individualizar la cuenta sobre la que se pide información mediante algún identificador válido.
- Indicar la fecha de visualización del perfil.
- Mencionar las fechas entre las cuales se requiere que se informe las direcciones IP de acceso
- Descripción del hecho y calificación legal con mención de la norma específica.

- Relación de la cuenta con la investigación, especificando a quien pertenece (víctima/imputado/tercero) y qué se pretende obtener de ella (por ejemplo, información para localizar al imputado, o prueba del hecho, etc.)
- Deberá estar fechado y contar con la firma y el sello del/la juez/a que emite la orden y el sello del tribunal. Facebook no procesa oficios firmados electrónicamente, ni que carezcan de fecha o sellos.

## INFORMACIÓN ADICIONAL.

- Si se solicita información de suscriptor por oficio o de contenido a través de canales diplomáticos, recomendamos preservar previamente los registros e indicar en el documento el número de caso otorgado a la preservación.
- Incluso en casos de emergencia, Facebook no brindará información de contenido a autoridades extranjeras. Si es necesario obtener específicamente ese tipo de datos debe recurrirse a redes de cooperación internacional.
- Los identificadores válidos de las cuentas de Facebook son el URL de la cuenta (facebook.com/LACUENTA), su dirección de email asociada, el teléfono celular asociado con código país y código de área y/o el número de identificación de la cuenta (ID). El nombre de usuario (@LACUENTA o "LA CUENTA") no es un identificador válido.
- Los identificadores válidos de las cuentas de Instagram varían dependiendo el caso pueden ser el URL de la cuenta (Instagram.com/LACUENTA), o el nombre usuario (@LACUENTA) o el número de identificación de la cuenta (ID) y/o el email o celular asociados (con código país y código de área)
- En ambos casos, cuando el identificador sea un número telefónico, la línea debe identificarse con el símbolo +, seguido del código país (54), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones. Ello, a efectos de no confundir una línea telefónica con el número de ID de una cuenta.
- Es importante gestionar las preservaciones y los pedidos de información ajustando la fecha del pedido a la de efectiva actuación del perfil en el caso ya que los datos pueden variar con el transcurso del tiempo. Incluso para el caso de un perfil no disponible en la actualidad, pueden recuperarse datos si se coloca la fecha en la que efectivamente fue utilizado.

# II. Google

## II. GOOGLE LLC.

Google LLC es propietaria de un gran número de productos a los que los usuarios de Internet acceden diariamente, siendo los más comunes Gmail y Youtube.

La experiencia dicta que podrá solicitarse la preservación de datos o entrega voluntaria de información de cualquier producto de la compañía si se cuenta con un identificador válido (correo electrónico, teléfono, ID, y/o URL).

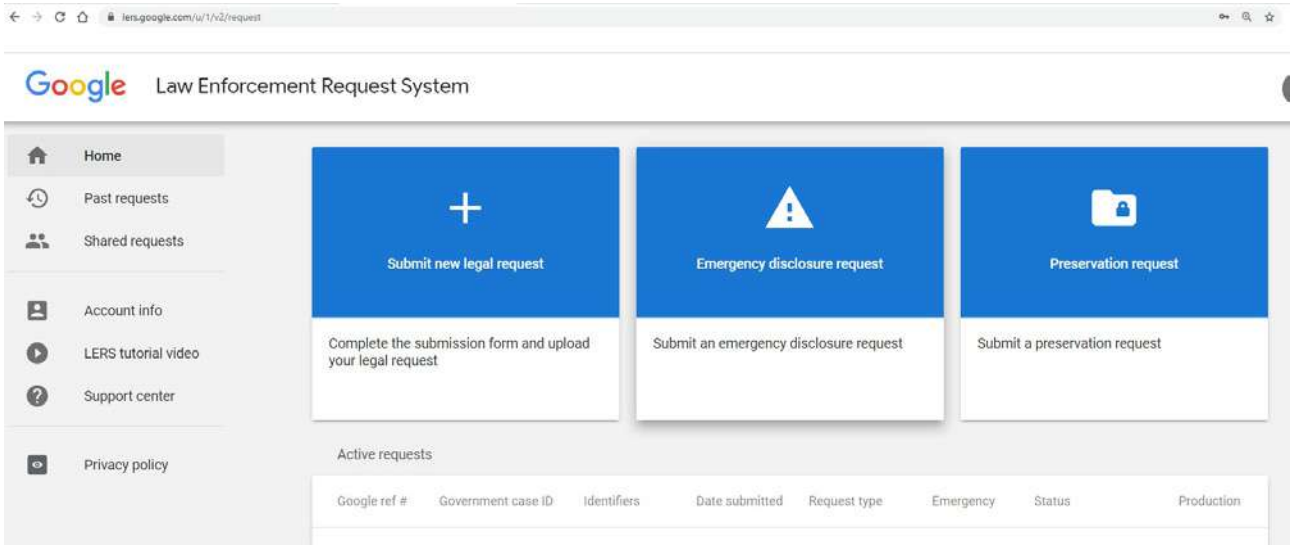
Sin embargo, hay ciertos productos sobre los cuales la empresa no preserva ni brinda información por las vías que señalaremos a continuación, por ejemplo, Google *Ads*.

### DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos se canalizan exclusivamente a través del portal *Law Enforcement Request System* (LERS), al que puede accederse a través del siguiente URL:

**https://lers.google.com/**

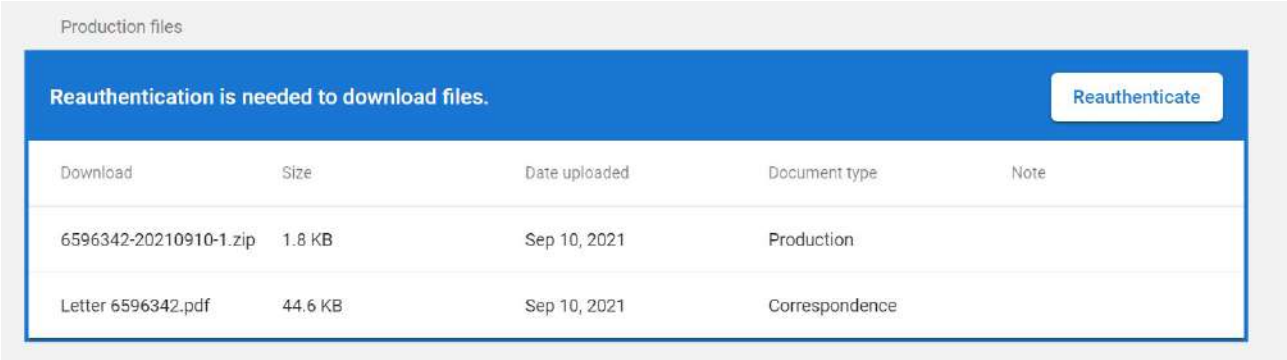
Google ha sido designado algunos puntos de contacto (*Google LERS single point of contact* - SPOC) para, entre otras cosas, presentar cuentas nuevas para su acreditación. En función de ello, aquellas dependencias que deseen tener su propia cuenta, para poder diligenciar sus oficios, podrán solicitárselo al SPOC que corresponda a su jurisdicción.



Para solicitar la **preservación** de datos y/o la **entrega voluntaria de información básica** del suscriptor ha de diligenciarse un oficio solicitando la medida (ver más abajo las formalidades con las que debe cumplirse). Al enviar el pedido a través del portal recibirá un email de confirmación con el número de caso y, cuando la información sea procesada, recibirá otro haciéndoselo saber.

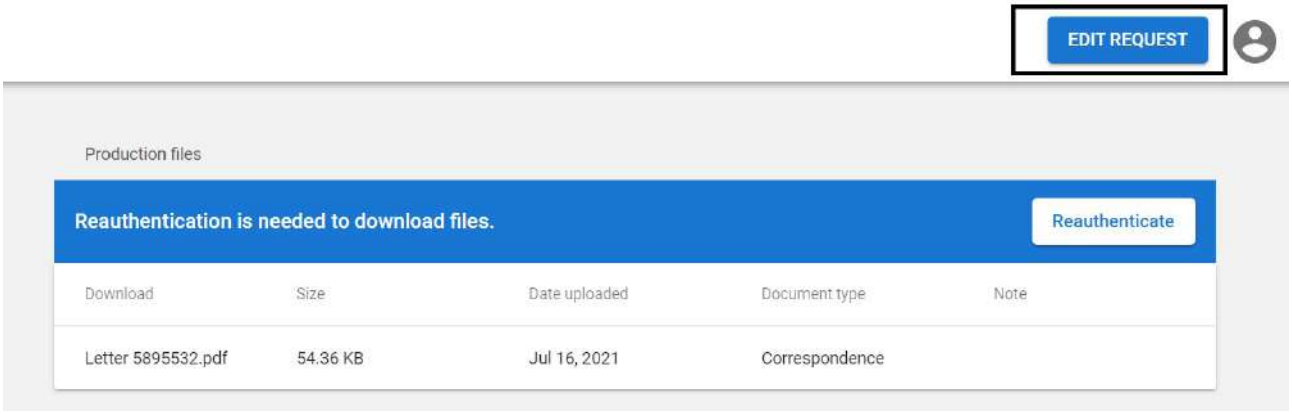
Si se trató de una preservación, podrá descargar un documento en formato .pdf con la confirmación o denegación de la medida.

Si se trató de información de suscriptor, además del citado documento se podrá descargar un archivo comprimido con la información, en general, en un archivo .txt y en otro archivo .html.




Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. Aconsejamos siempre dejar constancia de todo ese procedimiento.

En términos generales, Google preserva los registros por el plazo de 1 año. Los pedidos de **extensión de preservación** deben realizarse previo a la fecha de vencimiento de la medida editando el caso original y adjuntando un documento solicitando la medida. A diferencia de otras medidas, al enviar el pedido a través del portal NO recibirá un email de confirmación. Sólo recibirá un correo una vez que su solicitud sea procesada, y la respuesta esté disponible para ser descargada.



En los casos de **revelación de contenido de emergencia** (se considera emergencia cuando existe un peligro cierto y actual a la vida o a la integridad física) debe llenarse un formulario con preguntas relativas al tipo de caso, la naturaleza de la emergencia, la información deseada, etc. y acompañarse los documentos que permitan respaldar las afirmaciones (capturas de pantalla, fotografías, etc.). El formulario puede ser descargado del Portal y debe ser completado en inglés. Estas solicitudes pueden realizarse desde la cuenta de la Fiscalía o del Juzgado.

## FORMALIDADES DE LOS PEDIDOS.

Les detallamos los requisitos bajo los cuales la empresa accede a entregar información de suscriptor a autoridades de aplicación de la ley ubicadas fuera de los Estados Unidos.

El pedido debe:

- Estar dirigido a **Google, LLC, 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA**.
- Tener indicación de fecha, datos de la causa (autoridad judicial que solicita la información y tribunal).
- Especificar la cuenta con un identificador válido.
- Detallar la información que se pide.
- Precisar dirección a donde deberá enviarse la información solicitada (domicilio, nombre completo, dependencia, cargo, correo electrónico, teléfono y fax).
- Tener firma y sello de la autoridad requirente. Las solicitudes de preservación pueden ser firmadas por el/la fiscal/a del caso y las de entrega voluntaria de información de suscriptor por el/la juez/a. La empresa admite, para procesar los pedidos, firma ológrafa acompañada siempre por el sello del organismo o digital, no electrónica.

## INFORMACIÓN ADICIONAL.

- Si se solicita información a través de canales diplomáticos, recomendamos previamente preservar los registros. Google, además, solicita se informe en el requerimiento de asistencia el número de caso asignado a la preservación.
- Incluso en casos de emergencia, Google no brindará información de contenido a autoridades extranjeras. Si es necesario obtener específicamente ese tipo de datos debe recurrirse a redes de cooperación internacional.
- Cuando el dato que se posee es un número telefónico al que esta o podría estar asociado la cuenta de correo, informamos que las líneas deben identificarse con el símbolo +, seguido del código país (53), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones.

# III. Microsoft Corporation

## III. MICROSOFT CORPORATION.

Microsoft Co. es propietaria de un gran número de productos a los que los usuarios de Internet acceden diariamente, siendo los más comunes Hotmail, Skype, Outlook, Xbox, etc.

Tal como surge de la Guía para Solicitudes de Acceso a Datos por parte de Autoridades Competentes en América Latina Microsoft podrá proporcionar los siguientes registros:

**Datos de cuenta Microsoft:**

- Detalles de registro (información obtenida al momento de registro de la cuenta).
- Información de cobro (puede incluir dirección y medio(s) de pago).
- Transacciones de cobro (Tratado de Asistencia Mutua – "MLAT" por sus siglas en inglés).
- Registros IP (direcciones IP obtenidas al momento de inicio de sesión del usuario a un servicio específico).
- Correo electrónico alternativo y/o alias.
- Servicios utilizados.

**Datos de servicio de correo electrónico:**

- Detalles de registro (información obtenida al momento de registrar la cuenta).
- Registros IP (dirección IP utilizada al momento de iniciar sesión al servicio de correo electrónico).
- Encabezados en correo electrónico (requiere MLAT).
- Contenido del correo electrónico (requiere MLAT).
- Contactos de correo electrónico (MLAT).

**Datos de servicio de XBOX:**

- Detalles de registro (información obtenida al momento de registro de la cuenta).
- Número de serial o Gamertag.
- Registros IP (direcciones IP obtenidas al momento de iniciar sesión en algún servicio XBOX).
- Historial de cambio de Gamertag (requiere MLAT).
- Contactos de XBOX (requiere MLAT).
- Historial de juegos en línea de XBOX (requiere MLAT).
- Comunicaciones almacenadas (requiere MLAT).

**Datos de servicio OneDrive:**

- Detalles de registro (información obtenida al momento de registro de la cuenta).
- Registros IP (direcciones IP obtenidas al momento de iniciar sesión en algún servicio OneDrive).
- Archivos almacenados (requiere MLAT).
- Registro de transacciones (requiere MLAT).

**Datos del servicio de Skype:**

- Detalles de registro (obtenidos al momento de registrar la cuenta).
- Dirección de facturación (dirección de facturación provista por el usuario).
- Método de pago / Instrument Data.
- Registros IP (dirección IP utilizada al momento de iniciar sesión al servicio de correo electrónico).
- Historial de números de servicio de Skype (lista de número(s) de Skype asociados a un usuario).
- Registros de llamas Skype Out (historial de llamadas hechas a una línea adscrita a una Red Telefónica Pública Conmutada).
- Registros de Skype Numbers (historial de llamadas recibidas de una línea adscrita a una Red Telefónica Pública Conmutada).
- Historial de compras (datos de transacciones) (requiere MLAT).
- Datos de SMS (Historial de detalle de SMS) (requiere MLAT).
- Datos de correo electrónico (datos históricos de cambio de correo electrónico) (requiere MLAT).
- Lista de contactos del nombre de usuario de Skype (requiere MLAT).
- Contenido de chats/media del usuario de Skype (requiere MLAT).

**La empresa indica que son identificadores válidos a los efectos de realizar búsquedas de datos sensibles:**

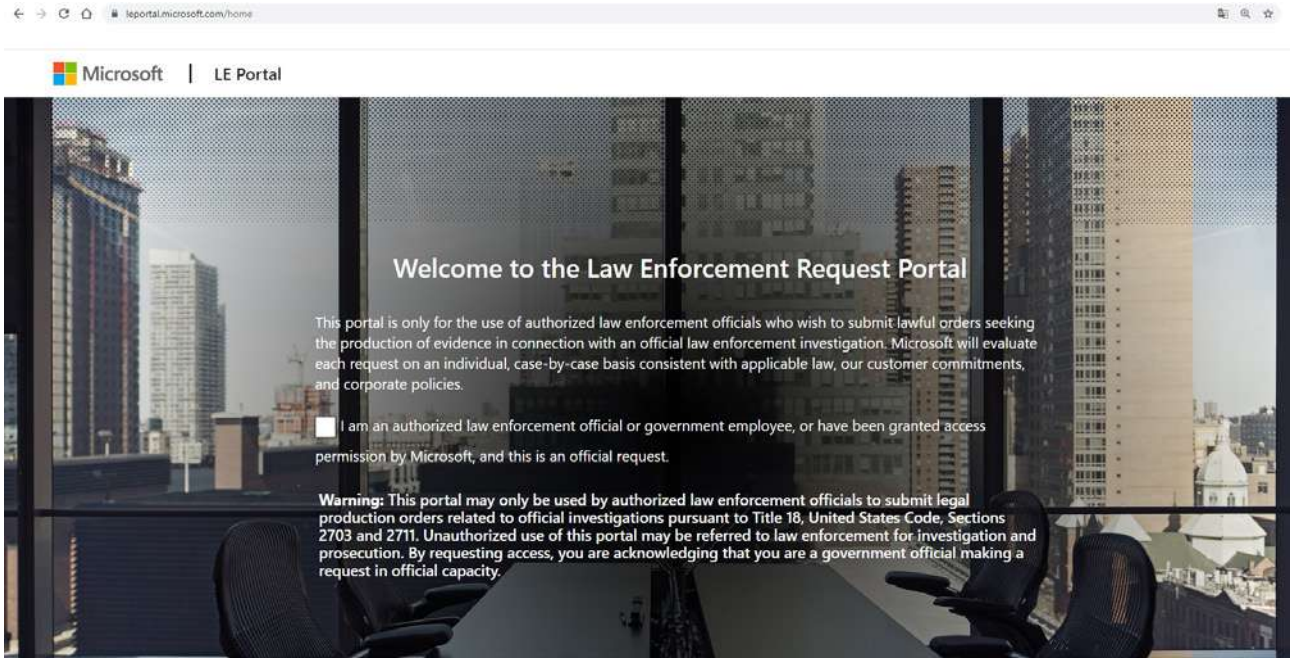
- Dirección de correo electrónico / Cuenta Microsoft (MSA).
- Número de teléfono (MSA).
- CID o PUID.
- Número de tarjeta de crédito (número completo).
- Xbox Gamertag, número de serie o tarjeta 5x5.
- Nombre de usuario / ID de Skype.
- Número de Skype acompañado de un intervalo de fechas específico.
- Número PSTN acompañado de una fecha y hora específicas y la duración de la llamada.
- Número de orden de Skype.

Todos los números de teléfono deben incluir el Código Internacional del País.

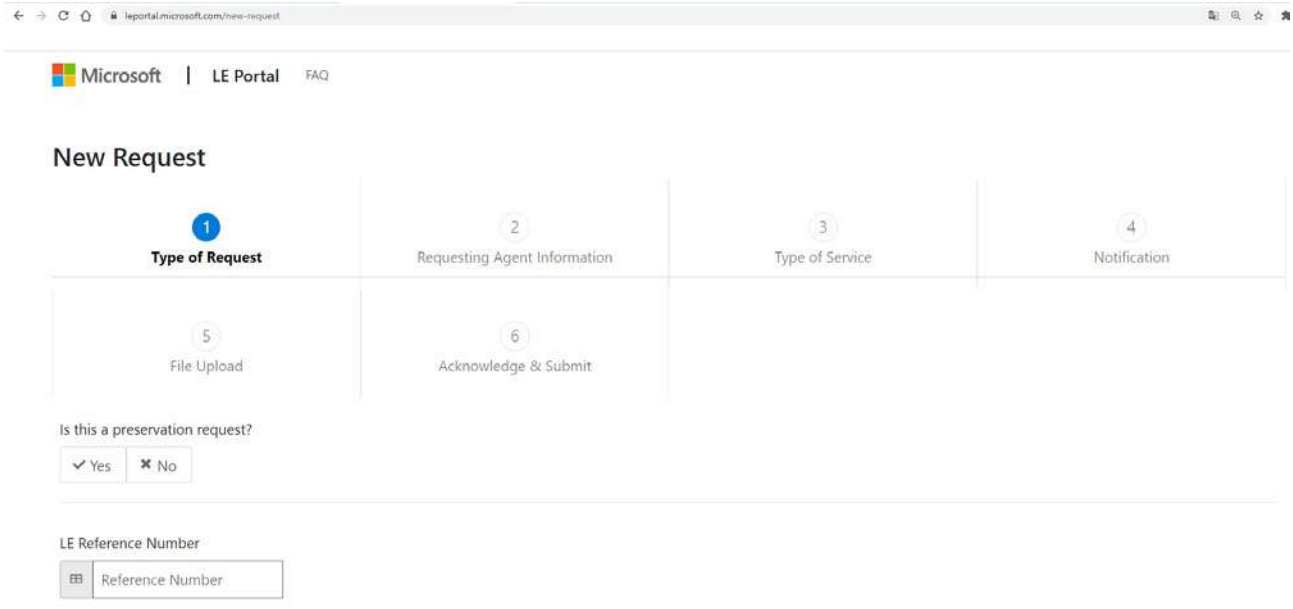
## DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos se canalizan exclusivamente a través del portal *Law Enforcement Request Portal (LE Portal)*, al que puede accederse a través del siguiente URL:

**https://leportal.microsoft.com/**




Para acceder al portal es necesario, previamente, crearse una cuenta de Microsoft (MSA, en inglés, Microsoft Account) y luego asociarla a la cuenta oficial de la Fiscalía, Juzgado, o Funcionario a cargo que hará de enlace con la compañía a través de su casilla de correo institucional (respectivamente, podría ser, por ejemplo, fisaliaxx@outlook.com/fiscaliaxx@mpf.gov.ar). Esto es importante, puesto que todas las notificaciones vinculadas a los requerimientos de información serán enviadas al correo oficial asociado.



Para solicitar la **preservación de datos** y/o l**a entrega voluntaria de información básica del suscriptor** ha de diligenciarse un oficio solicitando la medida (ver más abajo las formalidades con las que debe cumplirse). Al enviar el pedido a través del portal recibirá un email de confirmación con el número de caso y, cuando la información sea procesada, recibirá otro haciéndoselo saber.

Si se trató de una preservación, posteriormente recibirá un correo electrónico informando que de existir registros en los servidores de la empresa en relación a la/s cuenta/s de interés, estos serán preservados por un período de 180 días contados a partir de una fecha determinada. Vencido el plazo, se podrá solicitar la **extensión de la preservación** diligenciando una nueva solicitud a través de dicho Portal.

También existe la posibilidad de que responda que no se encontraron registros de la cuenta.

Si se trata de información de suscriptor, la empresa comunicará si encontró o no la información requerida en sus servidores. En caso afirmativo, se podrá ingresar al portal antes mencionado para descargar la información, usualmente contenida en un archivo de extensión .zip que estará identificado con el número de caso. En el mismo Portal se proveerá la contraseña para acceder al archivo y el valor *hash* del mismo, calculado en función SHA-256 por la empresa.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*, a efectos de verificar que coincida con aquel aportado por la compañía. Aconsejamos siempre dejar constancia de todo ese procedimiento.

A diferencias de las solicitudes anteriores, Microsoft responderá a los requerimientos de **revelación de contenido de emergencia** (se considera emergencia cuando existe un peligro cierto y actual a la vida o a la integridad física) a través del correo electrónico **LEALERT@microsoft.com**. La empresa considera como casos de emergencia situaciones tales como: secuestros, amenazas de asesinato, amenazas de bomba, amenazas de terrorismo, entre otras. Las solicitudes de emergencia deberán remitirse a la dirección de correo electrónico antes indicada, adjuntando nota escrita en idioma inglés, debidamente firmada, fechada y emitida en papel membretado de la Agencia o Autoridad Gubernamental de Aplicación de la Ley a la cual representa; indicando expresamente los motivos o razones por las cuales se considera de emergencia.

## FORMALIDADES DE LOS PEDIDOS.

De acuerdo a nuestra experiencia, cualquier pedido de preservación o de información básica del suscriptor que se le haga a la firma deberá dirigirse a **Legal and Corporate Affairs (LCA)-Microsoft Corporation USA, One Microsoft Way, Redmond, WA 98052, EE.UU, Fax: 954-492-1976.**

En el escrito sugerimos solicitar sólo aquella información que la empresa brinde de forma voluntaria (sin necesidad de rogatoria internacional o MLAT) en función del servicio específico sobre el que se está requiriendo.

Así, en relación a casillas de correo electrónico, por ejemplo, podrán solicitarse: (i) nombre y demás datos aportados al momento de crearse la cuenta, entre ellos, direcciones de correo electrónico y números de teléfono; (ii) fecha y hora de creación de la cuenta; (iii) dirección IP utilizada para crearla; (iv) direcciones de correo electrónico alternativas indicadas; (v) la totalidad de direcciones IP utilizadas para acceder a la cuenta que aún se encuentren conservadas en los servidores de la empresa, con indicación de fecha, hora y zona horaria del acceso; y en caso de existir, (vi) información de facturación (nombre, dirección, instrumento de pago y duración del servicio, incluyendo nombre del servicio).

La plataforma acepta que se suban otros documentos que sustancien el requerimiento en formato PDF, DOC, DOCX, XLS, o XLSX, con tamaño menor 25 MB, se sugiere escanear los oficios en formato .pdf.

**En relación al contenido, el pedido debe cumplir con los siguientes requisitos:**

- Estar dirigido a **Legal and Corporate Affairs (LCA)-Microsoft Corporation USA, One Microsoft Way, Redmond, WA 98052, EE.UU, Fax: 954-492-1976**.
- Estar confeccionada en papelería oficial;
- Tener indicación de fecha y datos de la causa (autoridad judicial que solicita la información y tribunal).
- Especificar la cuenta cuya información se requiere preservar o entregar información.
- Detallar el nombre, teléfono, dirección postal y dirección de correo electrónico del representante a quien la información debe ser enviada;
- Especificar el delito investigado con la cita de la norma en la que se encuentra tipificado (ej. Homicidio simple-art. 79 CP); y
- Estar firmada físicamente por la autoridad que emite la solicitud —ambas solicitudes pueden realizarlas tanto un Juez como un Fiscal—.

El oficio puede librarse en castellano. Nuestra experiencia indica que librar los pedidos en castellano, con su traducción en inglés, agiliza su procesamiento.

Al momento de diligenciar el oficio aparecerá la opción de notificar o no al usuario. Si se selecciona NO, la empresa requiere que se cite aquella legislación local que justifique la medida.

## INFORMACIÓN ADICIONAL.

- Si se solicita información a través de canales diplomáticos, recomendamos previamente preservar los registros. La empresa, además, solicita se informe en la solicitud de asistencia el número de caso asignado a la preservación.
- Las llamadas, mensajes automáticos y otras actividades entre usuarios de Skype no generan registros de facturación.
- Todos los registros son fechados y sellados individualmente. Consulte las notas al pie de página para conocer las zonas horarias.
- En caso de requerir información adicional, puede contactar con representantes de Microsoft al correo electrónico **msnwwcc@microsoft.com**. Es preferible que remita las consultas desde una dirección oficial de correo electrónico, de Autoridad o Agencia de Gobierno.
- Cuando el dato que se posee es un número telefónico al que esta o podría estar asociado la cuenta de correo, informamos que las líneas deben identificarse con el símbolo +, seguido del código país (54), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones.

# IV. Tik Tok

## IV. TIK TOK

De acuerdo a su Guía para las fuerzas investigativas, la empresa resguarda cierta información respecto de sus usuarios. Sin embargo, aclara, que la lista no es exhaustiva y puede contar con más información:

- **Información básica del suscriptor:** Nombre de usuario de TikTok, correo electrónico o número telefónico utilizado para acceder a la plataforma; fecha de creación de la cuenta; dirección IP de creación; información sobre el dispositivo utilizado por el usuario.
- **Registros de direcciones IP de inicio y cierre de sesión.**
- **Información relativa a la interacción del usuario con la plataforma (no es contenido):** Logs de las interacciones -por tiempos determinados-; y fecha y hora de creación de un video.
- **Información de contenido:** videos, comentarios y mensajes directos.

Por otra parte, la empresa afirma que cualquier pedido que le sea enviado debe identificar al usuario por el nombre de usuario de TikTok (o URL); aunque la empresa reconoce también otros identificadores válidos: El identificador (ID) del usuario; número telefónico o correo electrónico asociados a la cuenta; o identificador (ID) del video. Asimismo, en la medida que sea posible, la empresa solicita una captura de pantalla del usuario o del video sobre el cual se está requiriendo la medida.

De acuerdo a nuestra experiencia, la empresa recibe solicitudes en idioma inglés y sólo provenientes de casillas de correo oficiales.

### DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos de preservación se canalizan exclusivamente por correo electrónico a **lert@tiktok.com**. El Asunto del correo debe decir *"Preservation Request"*.

El oficio debe cumplir con los siguientes requisitos:

- Estar dirigido a **TikTok Pte. Limited, 1 Raffles Quay, #19-11, South Tower, SINGAPORE 048583**.
- Enviarse en papel membretado no editable (preferentemente en un documento .pdf), con indicación de fecha, datos de la causa y autoridad judicial que solicita la información;
- Consignar el fundamento legal que autoriza a quien emite la solicitud a solicitar y recopilar información con el fin de prevenir, detectar o investigar delitos penales.
- Individualizar la cuenta con un identificador válido;
- Especificar qué información se desea preservar;
- Determinar una fecha (y, si es posible, una hora), o un rango de fechas que sea relevante para la solicitud (solo para datos históricos);
- Precisar una dirección de correo electrónico oficial a donde deberá enviarse la respuesta a la

medida requerida.

- Especificar el delito investigado con la cita de la norma en la que se encuentra tipificado (ej. Homicidio simple-art. 79 CP);
- Si no se desea que el usuario sea notificado de la medida, la empresa requiere que se cite aquella legislación local que justifique la no divulgación de la misma.
- Tener firma y sello de la autoridad requirente (en un formato no editable). Las solicitudes de preservación pueden ser firmadas por el/la fiscal/a del caso. La empresa admite, para procesar los pedidos, firma ológrafa acompañada siempre por el sello del organismo o digital, no electrónica.

Procesado que sea el requerimiento, la empresa enviará un correo electrónico confirmando o no la medida por un plazo de 90 días.

Es posible que TikTok no acepte múltiples solicitudes de extensión más allá de un período adicional de 90 días. De no enviar un pedido de extensión de la medida antes de que esta venza, la empresa afirma que podrá eliminar de sus registros la información cuando expire el período de preservación.

Por otra parte, TikTok asegura que no procesará solicitudes de preservación que sean demasiado amplias o inespecíficas. Además, la solicitud de conservación de datos debe incluir una declaración sobre los pasos que se están tomando para obtener la información preservada mediante una orden judicial u otro proceso legal.

La política fijada por TikTok Pte. Limited para dar respuesta a los pedidos de asistencia formulados en el marco de investigaciones criminales en trámite ante países extranjeros, es únicamente dar a conocer información de sus usuarios cuando ésta sea requerida por medio de un proceso legal válido; es decir, que la petición sea hecha usando los procedimientos disponibles en virtud de un Tratado de Asistencia Legal Mutua (MLAT) o a través de una carta rogatoria.

Entonces, a diferencia de otras empresas que tienen una política distinta (Google o Facebook, por ejemplo) TikTok no entrega voluntariamente información a las autoridades extranjeras, ni siquiera la información de suscriptor.

La solicitud de asistencia legal debe ser firmada por el juez del caso y cumplir con los requisitos antes detallados. Deberán estar redactada de la forma más completa posible y contar con un detalle especifico de la información se requiere. Pedidos demasiado amplios, serán rechazados.

En los casos de **revelación de contenido de emergencia** (se considera emergencia cuando existe un peligro cierto y actual a la vida o a la integridad física), debe llenarse un formulario en inglés en línea (**https://www.tiktok.com/legal/report/EDR?lang=en**) con preguntas relativas al tipo de caso, la naturaleza de la emergencia, la información deseada, etc. al que se adjuntará los documentos que permitan respaldar las afirmaciones (capturas de pantalla, fotografías, etc.). El formulario puede ser

completado en inglés.

Por otra parte, podrá enviarse dicha solicitud por correo electrónico a lert@tiktok.com, el Asunto del correo debe decir "*Emergency Disclosure Request*". En ese caso, deberá acompañarse al pedido un oficio, que debe cumplir con las siguientes formalidades:

- Estar dirigido a TikTok Pte. Limited, 1 Raffles Quay, #19-11, South Tower, SINGAPORE 048583.
- Debe estar encabezado con el membrete (no editable) de la autoridad y/o organismo.
- Identificar a la persona que se encuentra en peligro de muerte o de sufrir un serio daño físico inminente.
- Individualizar la naturaleza de la emergencia (por ejemplo, posible caso de suicidio, ataque terrorista, amenaza de bomba, etc.);
- Identificar la cuenta sobre la que se pide información mediante algún identificador válido, incluyendo una captura de pantalla de la cuenta y, en caso contrario, una explicación de por qué no se adjunta.
- Aportar toda la información específica relativa a la emergencia y fundamentar por qué la información requerida es necesaria para prevenirla
- Tener firma y sello de la autoridad requirente (en un formato no editable). La empresa admite, para procesar los pedidos, firma ológrafa acompañada siempre por el sello del organismo o digital, no electrónica.

## INFORMACIÓN ADICIONAL.

Pueden encontrar más información en las "Directrices para organismos de seguridad" de Tiktok:

**https://www.tiktok.com/legal/law-enforcement?lang=es**

- Cuando el dato que se posee es un número telefónico al que esta o podría estar asociado la cuenta de TikTok, informamos que las líneas deben identificarse con el símbolo +, seguido del código país (52), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones.
- Si se solicita información a través de canales diplomáticos, recomendamos preservar previamente los registros e indicar en el documento el número de caso otorgado a la preservación.
- Es importante gestionar las preservaciones y los pedidos de información ajustando la fecha del pedido a la de efectiva actuación de la cuenta en el caso ya que los datos pueden variar con el transcurso del tiempo. Incluso para el caso de una cuenta no disponible en la actualidad, pueden recuperarse datos si se coloca la fecha en la que efectivamente fue utilizado.

# V. Twitter Inc.

## V. TWITTER INC.

Para efectuar pedidos a Twitter deberá consignarse el @nombredeusuario, el URL del perfil de Twitter correspondiente (p. ej., https://twitter.com/twittersafety [@twittersafety]), o el número de identificación de usuario único público de la cuenta de Twitter.

Asimismo, podrán solicitarse las medidas que se describirán a continuación en relación a direcciones de correo electrónico o números telefónicos que se presumen asociados a una cuenta de Twitter.

De acuerdo a los términos del servicio de la empresa, las cuentas de Twitter son, por defecto, públicas (cualquiera puede ver las publicaciones, incluso si no está suscripto a la red); pero el usuario tiene la opción de comunicarse de manera privada con otros usuarios o controlar quién ve su contenido.

### DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos se canalizan exclusivamente a través del portal *Legal Request Submissions Site*, al que puede accederse a través del siguiente URL:

**http://legalrequests.twitter.com**

El portal exige registrarse la primera vez que se ingresa, luego de lo cual sólo tendrá que ingresarse el correo de la fiscalía para recibir el enlace de ingreso, cuya vigencia es de una hora.

A través de dicha plataforma se pueden cursar pedidos de **preservación** llenando el formulario en línea y acompañando un oficio solicitando la medida. Al cargar una preservación, el sistema solicita que se especifique las fechas entre las cuales se desea conservar los datos. Asimismo, en dicha oportunidad, deberá especificarse qué información desea ser conservada (Información básica de la cuenta, IP de creación, Número de teléfono, Registros de sesiones IP, los Tweets, Mensajes directos, Multimedia, y/u otra información –en cuyo caso deberá especificarse cuál-).


El oficio debe cumplir con los siguientes requisitos:

- Estar dirigido a **Twitter, Inc. c/o Trust & Safety - Legal Policy, 1355 Market Street, Suite 900, San Francisco, CA 94103, USA**.
- Enviarse en papel membretado no editable (preferentemente en un documento .pdf), con indicación de fecha, datos de la causa y autoridad judicial que solicita la información.
- Especificar la cuenta con un identificador válido.
- Precisar una dirección de correo electrónico oficial a donde deberá enviarse la respuesta a la medida requerida.
- Tener firma y sello de la autoridad requirente (en un formato no editable). Las solicitudes de preservación pueden ser firmadas por el/la fiscal/a del caso. La empresa admite, para procesar los pedidos, firma ológrafa acompañada siempre por el sello del organismo o digital, no electrónica.

Al enviar el pedido a través del portal recibirá un correo electrónico de confirmación de recepción del pedido con el número de caso. Luego, se recibirá otro correo confirmando o no la medida.

Twitter preserva registros por 90 días, la empresa contempla la posibilidad de extender las preservaciones más de una vez. Bastará simplemente con enviar un pedido requiriéndolo -con al menos 7 días de antelación al vencimiento de la medida- que deberá cumplir con los requisitos detallados anteriormente y ser diligenciado a través del portal.

La política fijada por Twitter para dar respuesta a los pedidos de asistencia formulados en el marco de investigaciones criminales en trámite ante países extranjeros, es únicamente dar a conocer información de sus usuarios cuando ésta sea requerida por medio de un proceso legal válido; es decir, que la petición sea hecha usando los procedimientos disponibles en virtud de un Tratado de Asistencia Legal Mutua (MLAT) o a través de una carta rogatoria.

Entonces, a diferencia de otras empresas que tienen una política distinta (Google o Facebook, por ejemplo) Twitter no entrega voluntariamente información a las autoridades extranjeras, ni siquiera la información de suscriptor.

La solicitud de asistencia legal debe ser firmada por el juez del caso y enviada a las autoridades de los Estados Unidos para que, a su vez, emita orden judicial dirigida las oficinas **Twitter, Inc. c/o Trust & Safety - Legal Policy 94103 ubicadas en 1355 Market Street, Suite 900, San Francisco, CA 94103, United States of America**.

En los casos de **revelación de contenido de emergencia** (se considera emergencia cuando existe un peligro cierto y actual a la vida o a la integridad física), debe llenarse un formulario con preguntas relativas al tipo de caso, la naturaleza de la emergencia, la información deseada, etc. al que se adjuntará los documentos que permitan respaldar las afirmaciones (capturas de pantalla, fotografías, etc.). El formulario puede ser completado en castellano o en inglés. Asimismo, deberá acompañarse al pedido un oficio, que debe cumplir con las siguientes formalidades:

- Titular el pedido como Emergency Disclosure Request;
- Estar dirigido a **Twitter, Inc. c/o Trust & Safety - Legal Policy, 1355 Market Street, Suite 900, San Francisco, CA 94103, USA**.
- Debe estar encabezado con el membrete (no editable) de la autoridad y/o organismo.
- Identificar a la persona que se encuentra en peligro de muerte o de sufrir un serio daño físico inminente.
- Individualizar la naturaleza de la emergencia (por ejemplo, posible caso de suicidio, ataque terrorista, amenaza de bomba, etc.)
- Identificar la cuenta sobre la que se pide información mediante algún identificador válido
- De aplicar, detallar el tweet o tweets que le empresa debe revisar.

- Aportar toda la información específica relativa a la emergencia y fundamentar porque la información requerida es necesaria para prevenirla
- Tener firma y sello de la autoridad requirente (en un formato no editable). La empresa admite, para procesar los pedidos, firma ológrafa acompañada siempre por el sello del organismo o digital, no electrónica.

Al enviar un pedido de revelación de contenido de emergencia recibirá un email de confirmación de la recepción del pedido y, cuando la información sea procesada, recibirá otro con un link para descargarla.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. Aconsejamos siempre dejar constancia de todo ese procedimiento.


Por último, Twitter prevé dos mecanismos para la **solicitud de eliminación de contenido**.

En primer lugar, si el Tweet, Lista o Mensaje Directo incumple las Reglas de Twitter (https://help.twitter.com/es/rules-and-policies/twitter-rules), la empresa establece que tanto los agentes de policía como los funcionarios gubernamentales pueden solicitar que se revise y elimine el contenido potencialmente ilegal de Twitter por incumplir las leyes locales. La empresa detalla los pasos a seguir para cada caso en la siguiente página web: https://help.twitter.com/es/rules-and-policies/twitter-report-violation.

Si el pedido de revisión es rechazado, se puede enviar un requerimiento jurídico válido y correctamente definido para solicitar que se retenga el contenido. Twitter aclara que no deberá enviarse un requerimiento para retener contenido si este no fue previamente denunciado para una revisión de posible incumplimiento de sus Términos de Servicio.

En el portal la empresa ha habilitado un formulario para requerir la retención de contenido. Al completarlo deberá especificarse el tipo de causa (Civil o Penal), su naturaleza (Explotación sexual infantil, Violación del copyright, Infracción de las leyes de marca comercial, Amenazas violentas o instigación, Acoso, Información privada, Suplantación de identidad, Contenido gráfico, Difamación, Información confidencial, Infracción del derecho a la privacidad, Conductas de incitación al odio, Contenido ilegal, Otros –en cuyo caso deberá especificarse-), fundamento legal que respalde el requerimiento, y cualquier otra información adicional que robustezca el pedido. Por último, deberá adjuntarse la orden judicial ordenando la medida y cualquier otra documentación respaldatoria.

Si bien la empresa no lo exige, sí aclara que si la documentación es subida en idioma inglés será procesada más rápidamente.

En términos generales, Twitter notifica a sus usuarios sobre los requerimientos de información y retención de contenido y les proporciona una copia de la notificación judicial, a menos que el contenido denunciado incumpla los Términos de servicio de Twitter o que se prohíba notificar al usuario. Atento a ello, sugerimos que en sus oficios, siempre soliciten a la firma que no notifique al usuario.

Cuando un contenido determinado está retenido, los usuarios ven un mensaje con el texto “Tweet retenido” o “Cuenta retenida” en lugar del contenido denunciado.

Por otra parte, Twitter colabora con la firma Lumen para publicar requerimientos judiciales de eliminación de contenido, a menos que el contenido denunciado incumpla los Términos de servicio de Twitter o que se prohíba notificar a Lumen.

## INFORMACIÓN ADICIONAL.

- Pueden encontrar más información en las “Directrices para la policía” de Twitter: **https://help.twitter.com/es/rules-and-policies/twitter-law-enforcement-support.**
- Cuando el dato que se posee es un número telefónico al que esta o podría estar asociado la cuenta de Twitter, informamos que las líneas deben identificarse con el símbolo +, seguido del código país (59), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones.
- En relación a la plataforma Periscope (propiedad de Twitter Inc.), hacemos saber que Twitter eliminó el 31 de marzo de 2021 las aplicaciones de Periscope para iOS y Android. El sitio web de Periscope en periscope.tv permanecerá disponible como un archivo de solo lectura de las transmisiones públicas, pero no se podrá crear una nueva cuenta, transmitir en directo ni comprar monedas. Por ello, de desear obtener información en relación a cuentas en dicha plataforma, deberán seguirse los procedimientos anteriormente descriptos. Las cuentas de Periscope se identifican también por usuario y URL de Periscope (p. ej., @twittersafety y https://periscope.tv/twittersafety).

- La experiencia dicta que si el portal no admite la medida por no encontrar registros en sus servidores a partir del identificador seleccionado, ello puede deberse a que el usuario haya borrado su cuenta y consecuentemente la empresa la haya eliminado de sus registros, o que por inacción del usuario, Twitter haya adoptado dicho temperamento.
- Si se solicita información a través de canales diplomáticos, recomendamos preservar previamente los registros e indicar en el documento el número de caso otorgado a la preservación.
- Es importante gestionar las preservaciones y los pedidos de información ajustando la fecha del pedido a la de efectiva actuación de la cuenta en el caso ya que los datos pueden variar con el transcurso del tiempo. Incluso para el caso de una cuenta no disponible en la actualidad, pueden recuperarse datos si se coloca la fecha en la que efectivamente fue utilizado.

# VI. Whatsapp  LLC.

## VI. WHATSAPP LLC.

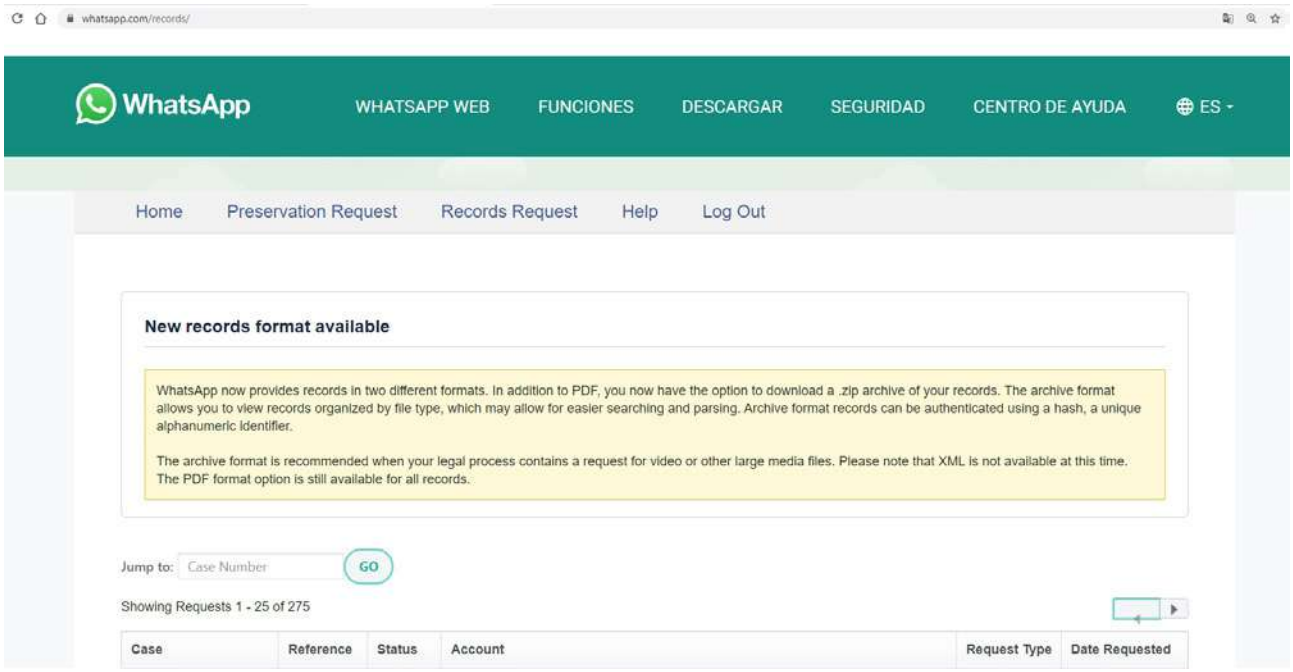
En primer lugar, hacemos saber que las medidas que se detallaran a continuación pueden realizarse respecto de números telefónicos y/o correos electrónicos asociados a cuentas de WhatsApp.

Las cuentas de WhatsApp corresponden a números telefónicos, principalmente de telefonía celular, pero también de telefonía fija. En el caso de números telefónicos las líneas deben identificarse con el símbolo +, seguido del código país (56), código de área o celular (según corresponda) y el número de la línea.

### DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos se canalizan exclusivamente a través del portal *Law Enforcement On Line Requests* (LEORS), al que puede accederse a través del siguiente URL:

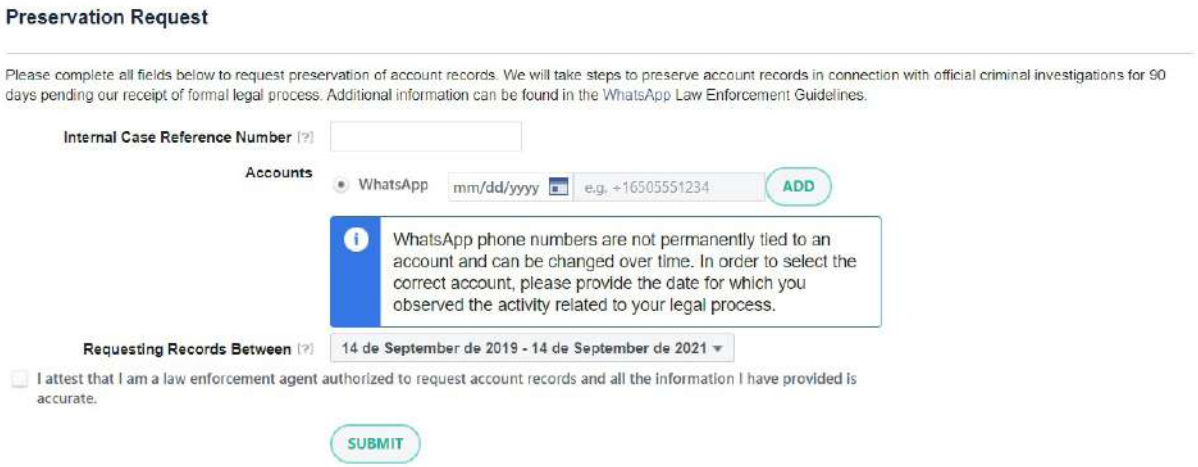
**https://www.whatsapp.com/records/**




El portal exige registrarse la primera vez que se ingresa, luego de lo cual sólo tendrá que ingresarse el correo de la fiscalía para recibir el enlace de ingreso, cuya vigencia es de una hora.

A través de dicha plataforma se pueden cursar pedidos de **preservación** llenando el formulario en línea

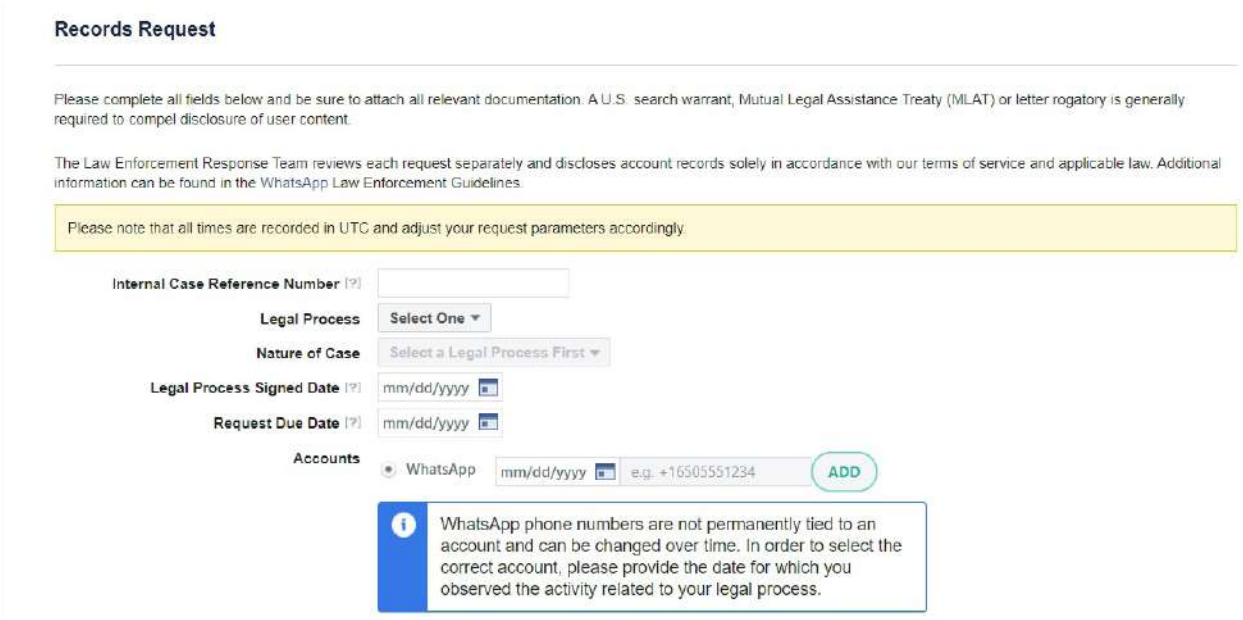
sin acompañar documentos. Al cargar una preservación, por defecto el sistema resguarda los registros de los últimos dos años. Si es necesario, puede elegirse un período de tiempo distinto (mayor o menor).

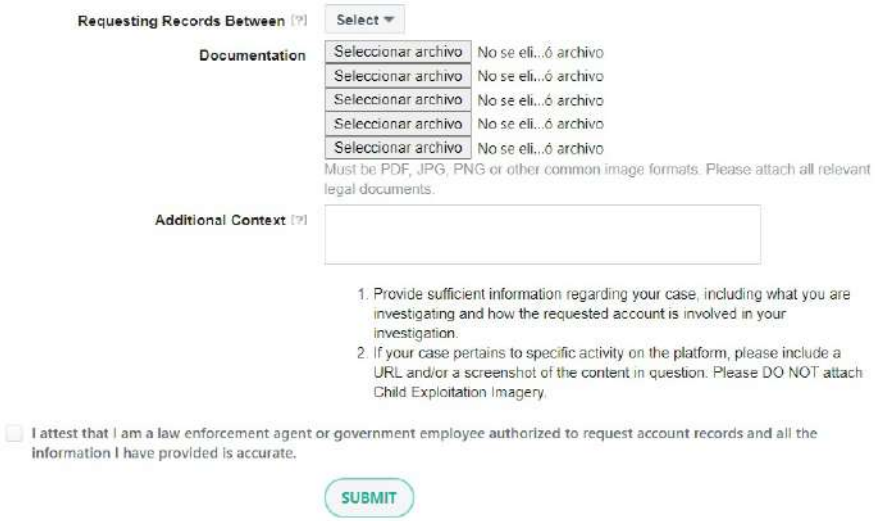



Al enviar el pedido de preservación recibirá un email de confirmación con el número de caso y podrá verificar a través del portal la fecha de vencimiento.

WhatsApp preserva registros por 90 días, aunque el **portal admite extender las preservaciones** más de una vez. Bastará simplemente con seleccionar el caso, la cuenta de interés y hacer *click* en el botón de extender.

Para los pedidos de **entrega voluntaria de información de suscriptor** deben completarse una serie de campos adicionales como el tipo de caso, la fecha de la orden judicial, el período de tiempo de los registros solicitados y debe acompañarse la solicitud en formato .pdf, que se detallan más abajo.






Aclaramos que WhatsApp solo brindará aquella información disponible en sus registros al momento de realizar la compulsa en función de un pedido de este estilo. Es decir, si la cuenta no se encontraba activa en dicha oportunidad, la empresa no brindará mucha información sobre la misma, mientras que si la cuenta sí estaba activa, puede que provea conexiones IP, correo electrónico asociado, modelo del dispositivo, sistema operativo, por ejemplo. Cualquier otra información, deberá solicitarse por la vía de rogatoria internacional.

En cualquier caso, sugerimos limitar el pedido a este tipo de información, por cuanto cualquier exceso en el mismo puede motivar un rechazo *in limine*.

En los casos de **revelación de contenido de emergencia** (se considera emergencia cuando existe un peligro cierto y actual a la vida o a la integridad física) debe llenarse un formulario con preguntas relativas al tipo de caso, la naturaleza de la emergencia, la información deseada, etc. y acompañarse los documentos que permitan respaldar las afirmaciones (capturas de pantalla, fotografías, etc.). El formulario puede ser completado en español o en inglés.

Al enviar un pedido de revelación de contenido de emergencia o de entrega voluntaria de información de suscriptor recibirá un *email* de confirmación de la recepción del pedido y, cuando la información sea procesada, recibirá otro haciéndoselo saber. A través del portal podrá descargar la información entregada en un archivo comprimido y en un documento en formato .pdf.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. En general, el portal informa el valor *hash* en formato SHA 256 del documento comprimido, no del .pdf. Aconsejamos siempre dejar constancia de todo ese procedimiento.

De acuerdo a nuestra experiencia, si el portal no admite la medida por no encontrar registros en sus servidores del identificador seleccionado, ello puede deberse a que el usuario haya borrado su cuenta y consecuentemente la empresa la haya eliminado de sus registros, o que por inacción del usuario, WhatsApp haya adoptado dicho temperamento. Es decir, si el identificador seleccionado no puede insertarse en el campo correspondiente, la empresa no admitirá la medida solicitada.

## FORMALIDADES DE LOS PEDIDOS.

Les detallamos los requisitos bajo los cuales la empresa accede a entregar información de suscriptor a autoridades de aplicación de la ley ubicadas fuera de los Estados Unidos.

Los pedidos pueden hacerse en castellano, recomendamos utilizar un lenguaje sencillo.

**El pedido debe:**

- Estar dirigido a **WhatsApp LLC, 1601 Willow Rd., Menlo Park, CA 94025, California, United States**,
- Indicar número de expediente
- Individualizar la cuenta sobre la que se pide información mediante algún identificador válido
- Indicar la fecha en la que la cuenta estuvo activa (Si es que pudo comprobarse)
- Descripción del hecho y calificación legal con mención de la norma específica.
- Relación de la cuenta con la investigación, especificando a quien pertenece (víctima/imputado/tercero) y qué se pretende obtener de ella (por ejemplo, información para localizar al imputado, o prueba del hecho, etc)
- Indicar con la fecha y lugar, y contar con la firma y el sello del/la juez/a que emite la orden y el sello del tribunal. WhatsApp no procesa oficios firmados electrónicamente, ni que carezcan de fecha o sellos.

## INFORMACIÓN ADICIONAL.

- Si se solicita información de suscriptor por oficio o de contenido a través de canales diplomáticos, recomendamos preservar previamente los registros e indicar en el documento el número de caso otorgado a la preservación.
- Incluso en casos de emergencia, WhatsApp no brindará información de contenido a autoridades extranjeras. Si es necesario obtener específicamente ese tipo de datos debe recurrirse a redes de cooperación internacional.
- Es importante gestionar las preservaciones y los pedidos de información ajustando la fecha del

pedido a la de efectiva actuación del perfil en el caso ya que los datos pueden variar con el transcurso del tiempo. Incluso para el caso de un perfil no disponible en la actualidad, pueden recuperarse datos si se coloca la fecha en la que efectivamente fue utilizado.

# VII. Yahoo! – AOL (Verizon Media)

## VII. YAHOO! – AOL (VERIZON MEDIA)

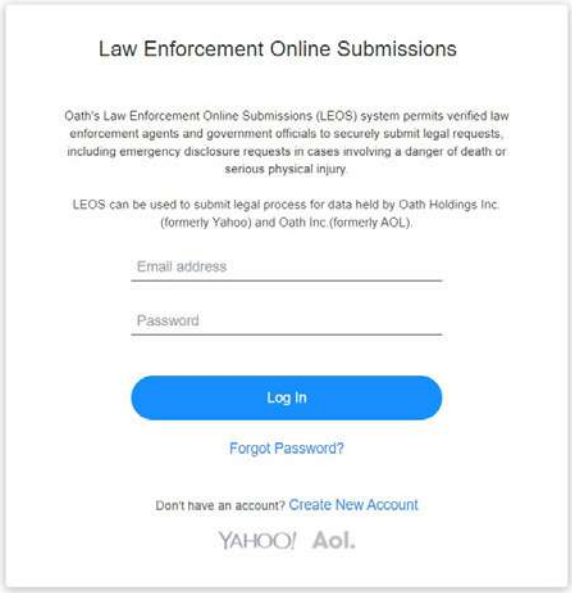
Yahoo Inc. es una empresa de tecnología multinacional estadounidense cuyo negocio se centra en los medios y los negocios en línea. Verizon Communications adquirió AOL en 2015. Cuando Verizon Communications compró Yahoo! en 2017, fusionó ambas empresas en una subsidiaria llamada Oath Inc.

Yahoo! es una plataforma de búsquedas que ofrece las últimas noticias, entretenimiento e información deportiva. La plataforma brinda acceso a otros servicios de la empresa, como ser: Yahoo! Aviate, Yahoo! Cine, Yahoo! Connected TV, Yahoo! Contactos, Correo Yahoo!, Flickr, Yahoo! Groups, Yahoo! Messenger, Yahoo! Móvil, Yahoo! Noticias, Yahoo! Search y Yahoo! Video.

### DILIGENCIAMIENTO DE PEDIDOS.

La empresa cuenta con un portal a través del cual pueden diligenciarse solicitudes. Se trata de del portal *Oath's Law Enforcement Online Submissions* (LEOS), al que puede accederse a través del siguiente URL:

**https://lawenforcementrequests.oath.com/**



El portal exige registrarse la primera vez que se ingresa. **Actualmente, la empresa no admite la registración de usuarios internacionales**. Por lo que cualquier requerimiento, deberá ser enviado por correo electrónico a **legalpoc@verizonmedia.com**.

Para solicitar la **preservación de datos** y/o la **entrega voluntaria de información básica del suscriptor** ha de diligenciarse un oficio solicitando la medida (ver más abajo las formalidades con las que debe cumplirse). Usualmente, tras enviar el pedido, recibirá por correo electrónico una respuesta automática de confirmación de recepción.

Si se trató de una preservación, recibirán un correo electrónico informando que de existir registros en los servidores de la empresa en relación a la/s cuenta/s de interés, estos serán preservados por un período de 90 días. Vencido el plazo, se podrá solicitar la **extensión de la preservación** enviando una nueva solicitud que referencie a la anterior. También existe la posibilidad de que responda que no se encontraron registros de la cuenta.

Si se trata de información de suscriptor, la empresa comunicará si encontró o no la información requerida en sus servidores. En caso afirmativo, adjuntará la respuesta al correo electrónico.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*, a efectos de verificar que coincida con aquel aportado por la compañía. Aconsejamos siempre dejar constancia de todo ese procedimiento.

Sin perjuicio de los antedicho, puede que la empresa responda que la información que se solicita o cuya preservación se busca sea administrada por alguna de sus filiales, como por ejemplo, **Verizon Media EMEA Limited**, con domicilio legal en 5-7 Point Square, N Wall Quay, North Dock, Dublin, D01 CF99, Irlanda, o **Verizon Media Hispanic Americas LLC**, que tiene domicilio legal en 1921 NW 87 Avenue, Doral, FL 33172, USA.

Consecuentemente, los pedidos deben dirigirse a la filial que se indique y por correo electrónico a la dirección que brinde Verizon.

## FORMALIDADES DE LOS PEDIDOS.

De acuerdo a nuestra experiencia, cualquier pedido de preservación o de información básica del suscriptor, debe cumplir con los siguientes requisitos:

- Estar dirigido a **Verizon Media International Inc., 1921 NW 87 Avenue, Doral, FL 33172, USA.**
- Estar confeccionada en papelería oficial;
- Tener indicación de fecha y datos de la causa (autoridad judicial que solicita la información y tribunal).

- Especificar la cuenta cuya información se requiere preservar o entregar información.
- Detallar el nombre, teléfono, dirección postal y dirección de correo electrónico del representante a quien la información debe ser enviada;
- Estar firmada físicamente por la autoridad que emite la solicitud.

El oficio puede librarse en castellano. Nuestra experiencia indica que librar los oficios en castellano, con su traducción en inglés, agiliza su procesamiento.

## INFORMACIÓN ADICIONAL.

- Si se solicita información a través de canales diplomáticos, recomendamos previamente preservar los registros.
- Son identificadores válidos para este tipo de pedidos el Yahoo! ID del usuario; la dirección de correo electrónico Yahoo! y/o AOL: XXXX@ymail.com, XXXX@rocketmail.com, XXXX@yahoo.com, o XXXX@aol.com; el número de identificación de usuario de Flickr (http://flickr.com/XXXXXXXX); o, el nombre de usuario del perfil de Flickr (http://flickr.com/photos/username)

# VIII. Uber

## VIII. UBER.

UBER TECHNOLOGIES INC. es una empresa estadounidense que proporciona a sus clientes a nivel internacional vehículos de transporte con conductor (VTC), a través de su software de aplicación móvil (app), que conecta los pasajeros con los conductores de vehículos registrados.

A diferencia de otras empresas, Uber permite a los Fiscales solicitar la preservación de información, como así también requerir información de suscriptor, tráfico y contenido, sin necesidad de orden emanada de un juez. Ello, por cuanto Uber ya cuenta de manera previa con la aceptación del usuario sobre el tratamiento de su información, en particular, en lo que respecta a su solicitud en el marco de investigaciones de índole penal.

La empresa podrá proporcionarle a los investigadores los siguientes tipos de información:

### Información del Suscriptor

**Con relación a los pasajeros:**

1. Nombre
2. Número de teléfono
3. Dirección de correo electrónico
4. Información bancaria
5. ID o identificación oficial

**Con relación a los socios (conductores/repartidores):**

1. Nombre
2. Número de teléfono
3. Dirección de correo electrónico
4. Información bancaria
5. Licencia
6. Foto de perfil
7. Información del vehículo

### Información de tráfico

**Con relación a los pasajeros:**

1. Fecha de inicio y término de uso del servicio

**Con relación a los viajes:**

1. Punto de inicio
2. Punto final
3. Recorrido
4. Fecha
5. Hora

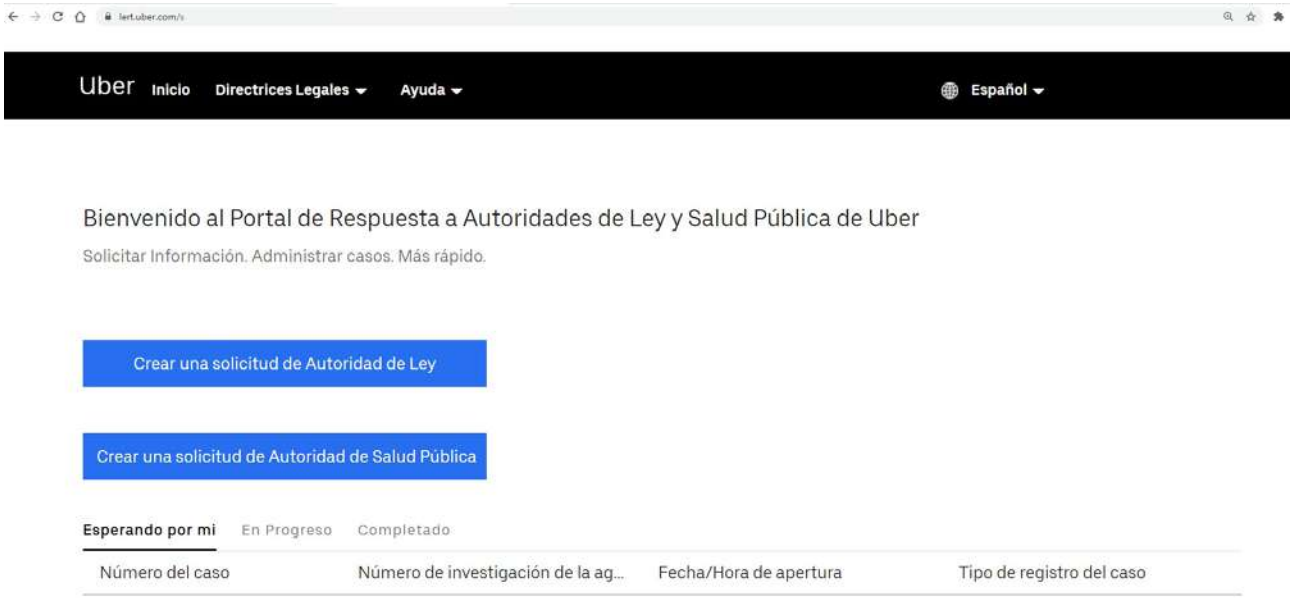
### Información de Contenido

Mensajes de texto entre usuarios conductores y repartidores.

## DILIGENCIAMIENTO DE PEDIDOS.

Los pedidos se canalizan exclusivamente a través del portal *Law Enforcement Request Portal (LE Portal)*, al que puede accederse a través del siguiente URL:

**https://lert.uber.com/**




El portal exige registrarse la primera vez que se ingresa, una vez que la empresa haya verificado la veracidad de los datos informados al momento de la registración y haya aprobado al usuario, sólo tendrá que ingresarse el correo y la clave para ingresar al Portal.

A través de dicha plataforma se pueden cursar pedidos de **preservación** llenando el formulario en línea. La empresa ofrece dos opciones para concretar la medida, una que requiere la carga de una solicitud librada por la autoridad competente (*"Si - Tengo un proceso legal y/o es una emergencia"*) y otra que no lo exige, pero que le solicitará que agregue información de al menos una persona, viaje, o vehículo (*"No - No tengo un proceso legal y quisiera realizar una solicitud de preservación"*)

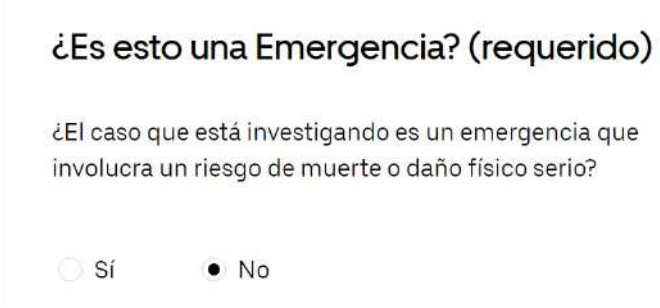

Al enviar el **pedido de preservación** recibirá un email de confirmación con el número de caso. Una vez procesada la solicitud, recibirá otro confirmando o denegando la medida. Uber preserva registros por 90 días.

Si se trata de un **pedido de información**, deberá completarse otro formulario con una serie de campos adicionales. Asimismo, es necesario adjuntar una orden emanada de autoridad compente. La empresa comunicará si encontró o no la información requerida en sus registros. En caso afirmativo, se podrá ingresar al Portal antes mencionado para descargar la información.

En muchos casos, la empresa brindará la contraseña para acceder a los archivos. Tenga presente que los mismos se encontrarán disponibles para su descarga por un tiempo limitado.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. Aconsejamos siempre dejar constancia de todo ese procedimiento.

Al momento de solicitar la preservación de información o su entrega, en los formularios a completar la empresa preguntar acerca de si el pedido es un **requerimiento de emergencia**. Pudiendo así canalizar este tipo de pedidos.




Por último, sugerimos consultar siempre el estado de sus requerimientos en el Portal. Hacemos saber que la empresa podrá requerir más información de su parte. En ese supuesto, el caso aparecerá en la sección "*Esperando por mi*". Cuando el caso se encuentre siendo procesado, podrá visualizarlo en la sección "*En Progreso*", una vez finalizado, pasará a la sección "*Completado*".

## FORMALIDADES DE LOS PEDIDOS.

De acuerdo a nuestra experiencia, el pedido debe cumplir con los siguientes requisitos:

- Estar dirigido a **Uber Technologies Inc., 1455 Market Street, San Francisco, CA, 94103, USA**.
- Estar confeccionada en papelería oficial;
- Tener indicación de lugar, fecha y datos de la causa o investigación;
- Detallar el nombre, teléfono, dirección postal y dirección de correo electrónico del representante a quien la información debe ser enviada;
- Breve descripción del hecho y calificación legal con mención de la norma específica.
- Relación de la cuenta con la investigación, especificando a quien pertenece (víctima/imputado/tercero) y qué se pretende obtener de ella (por ejemplo, información para localizar al imputado, o prueba del hecho, etc.)
- Para los pedidos de información, detallar la información se desea obtener de Uber (Es necesario ser lo más concreto posible con lo que se solicita y proporcionar la mayor información que permita la identificación tales como: Nombre completo/número de teléfono/correo electrónico/placas/fecha/hora y ubicación lo más exacta posible.)
- Tener firma y sello de la autoridad requirente.

El oficio puede librarse en castellano.

Sugerimos, de corresponder, requerir a la empresa que no notifique al usuario de la solicitud.

## INFORMACIÓN ADICIONAL.

- Si se solicita información a través del portal o por canales diplomáticos, recomendamos previamente preservar los registros.
- Cuando el dato que se posee es un número telefónico, informamos que las líneas deben identificarse con el símbolo +, seguido del código país (54), código de área o celular (según corresponda) y el número de la línea. Sin espacios, ni guiones.

# IX. Netflix B.V.

## IX. NETFLIX B.V.

Netflix International B.V. es un servicio que ofrece a sus suscriptores el acceso a películas, series de televisión y otras obras audiovisuales que se emiten por *streaming* a determinados televisores, ordenadores y otros dispositivos conectados a Internet. La suscripción a Netflix tiene carácter mensual.

Hacemos saber que la empresa coopera con las autoridades competentes **sólo en aquellas investigaciones penales relacionadas con dispositivos robados y el uso fraudulento de tarjetas de crédito**. En dichos casos, la empresa podrá revelar ciertos datos del propietario de una cuenta de Netflix o de su forma de pago.

Para el resto de las investigaciones penales, las autoridades que no estén ubicadas en los Países Bajos deben enviar la solicitud directamente a las autoridades judiciales de los Países Bajos conforme a los tratados que rigen las solicitudes de asistencia legal.

### DESCARGA DE INFORMACIÓN.

La empresa informa que sus usuarios pueden acceder a cierta información de interés para las investigaciones directamente desde su cuenta. En particular, el suscriptor puede ver la fecha y hora del *streaming*, junto con el país, estado y dirección IP desde donde se utilizó el servicio de *streaming*, y el tipo de dispositivo utilizado para verlo.

Para ello, el usuario deberá acceder a su cuenta "Cuenta", luego a la sección "Actividad reciente de *streaming* del dispositivo" dentro del apartado "Configuración".

Netflix aclara que en esa página solo se muestra información relacionada con dispositivos activos. Asimismo, debe tenerse presente que la ubicación es aproximada y se calcula según el lugar en el que esté registrada la dirección IP detectada.

Para más información puede consultarse el Centro de Ayuda de Netflix:

**https://help.netflix.com/support/1018.**

### FORMALIDADES Y DILIGENCIAMIENTO DE PEDIDOS.

A efectos de solicitar información, se debe completar el Formulario de Solicitud de datos por parte de la Autoridad Competente, disponible en el siguiente URL:

https://help.nflxext.com/legal/INTL_BV_Information_Request_Form_ES_LATAM.pdf

A efectos de identificar la cuenta objeto de investigación, la solicitud deberá incluir, al menos:

- La dirección de correo electrónico vinculada a la cuenta de Netflix; o,
- Información completa sobre la forma de pago relacionada con el fraude de cargos/pagos/tarjetas (número completo de la tarjeta de débito/crédito, IBAN o email de PayPal); o,
- Descripción de dispositivo(s) robado(s) (tipo, la marca y el tamaño de la pantalla).

Una vez completado el formulario, éste deberá ser firmado y sellado por la autoridad competente, y finalmente digitalizado en formato .pdf para ser enviado por correo electrónico a **legalprocess@netflix.com**. La empresa solo aceptará solicitudes enviadas por correo electrónico desde una dirección oficial de una autoridad competente.

Procesada que sea la solicitud, la empresa comunicará si encontró o no la información requerida en sus servidores. En caso afirmativo, adjuntará al correo la información que obre en sus registros. Al respecto, Netflix puede proporcionar los siguientes datos:

- **Información de la cuenta:** Nombre de la cuenta, dirección de correo electrónico, estado, número de cuenta de Netflix, país de suscripción, las 4 últimas cifras de la forma de pago registrada y el número de teléfono (si está disponible); y las 4 últimas cifras de todas las formas de pago asociadas a la cuenta y el historial de facturación (fecha e importe).
- **Direcciones IP de la forma de pago:** Las direcciones IP asociadas a los métodos de pago que ha añadido el suscriptor con marca de hora/fecha.
- **Lista de dispositivos:** Los dispositivos utilizados para ver por *streaming* los contenidos del servicio de Netflix.
- **Direcciones IP de *streaming*:** Las direcciones IP empleadas para acceder al servicio de Netflix y para ver sus contenidos a través de un dispositivo de *streaming* (consola de videojuegos, teléfono móvil, tableta, ordenador personal, TV conectado a Internet, reproductores de Blu-ray, etc.) con la marca de hora/fecha y el tipo de dispositivo.

# X. PayPal

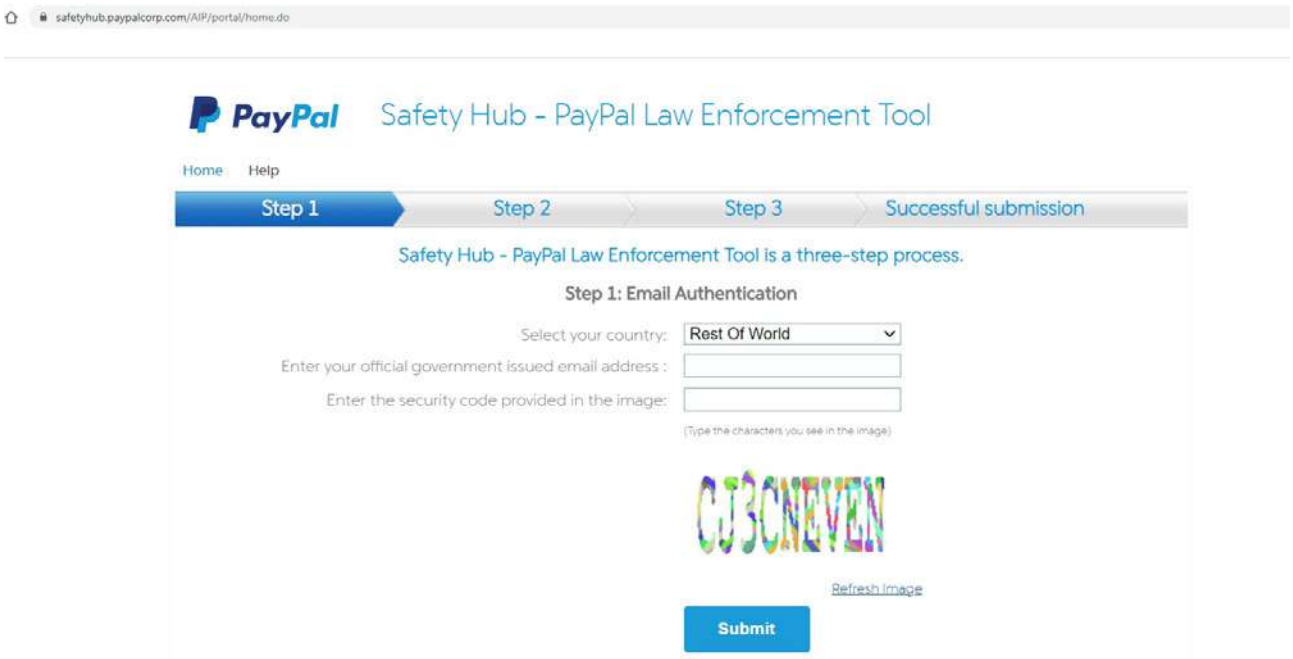
## X. PAYPAL

En términos generales, PayPal es un proveedor de servicios que opera un sistema de pagos y transferencias electrónicas de dinero entre sus usuarios.

### DILIGENCIAMIENTO DE PEDIDOS.

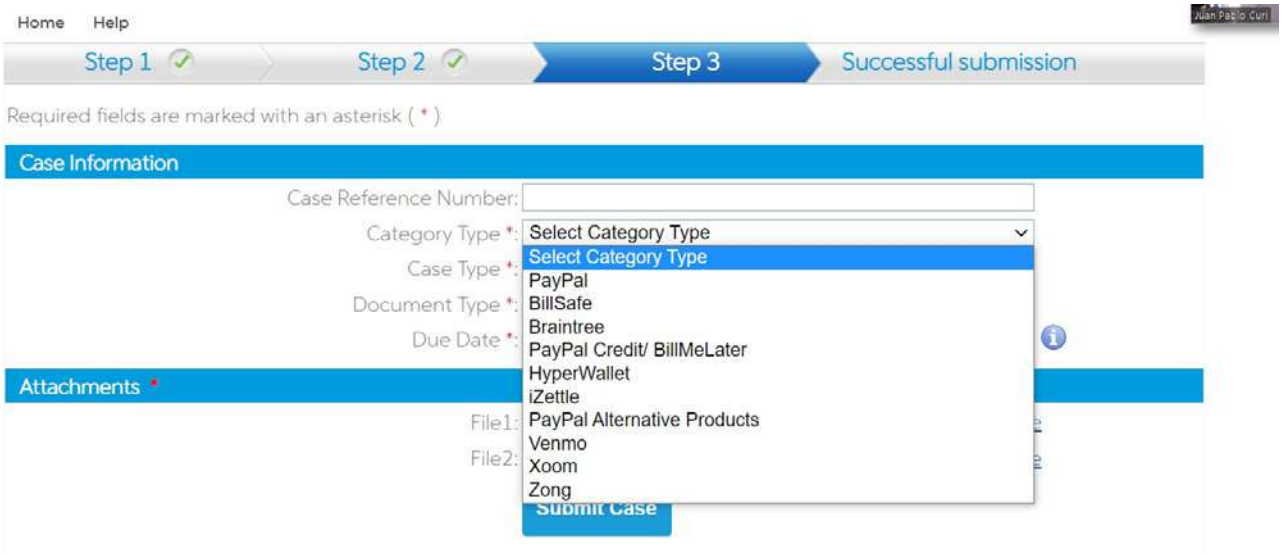
Los pedidos se canalizan exclusivamente a través del portal *Safety Hub - PayPal Law Enforcement Tool*, al que puede accederse a través del siguiente URL:

**https://safetyhub.paypalcorp.com/**

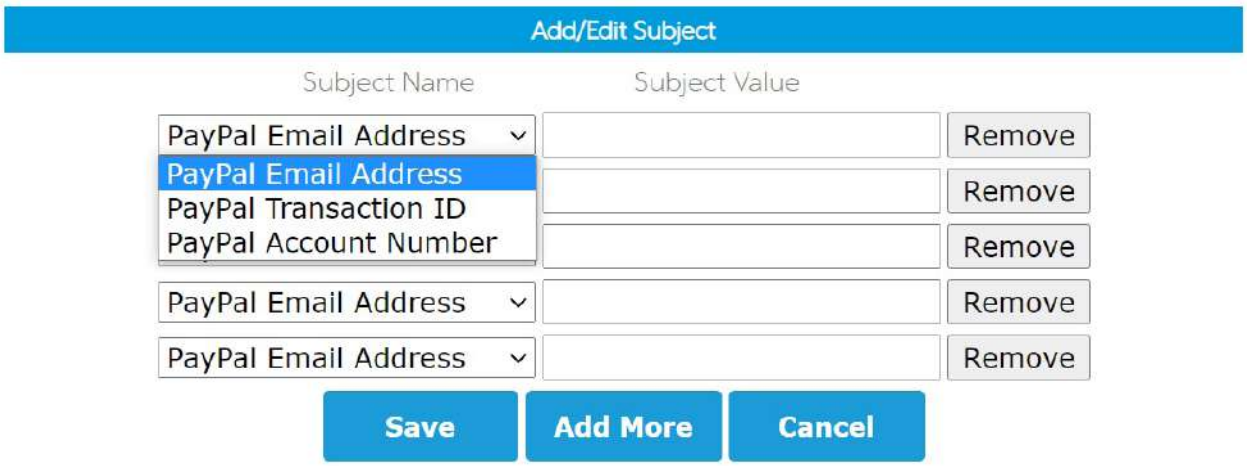



El portal exige registrarse la primera vez que se ingresa. Luego de lo cual sólo tendrá que ingresar el correo electrónico para recibir el enlace al portal.

Tras revalidar la casilla de correo, podrá realizarse un pedido de **entrega voluntaria de información** llenando el formulario en línea que variará dependiendo del servicio respecto del cual se quiere pedir información.




Si el servicio seleccionado es PayPal, el formulario requerirá que se consigne alguno de los siguientes identificadores: correo electrónico, ID de transacción o número de cuenta de PayPal.




Tras completar los campos obligatorios, se deberá adjuntar la solicitud dirigida a **PayPal Pte. Ltd. (Singapore)**, indicando qué información se desea obtener, firmada y sellada por la autoridad competente.

Los investigadores pueden solicitarle a la empresa: información básica del suscriptor; información sobre la tarjeta de crédito, débito, cuenta bancaria, etc.; información transaccional y direcciones IP.

Al enviar el pedido recibirá un email de confirmación de la recepción del pedido. Posteriormente, la empresa comunicará si encontró o no la información requerida en sus servidores. En caso afirmativo, brindará en el correo electrónico las instrucciones para descargar la información.

Recomendamos trabajar con una copia de esa información y guardar el original en una carpeta de evidencia luego de calcular su valor *hash*. Aconsejamos siempre dejar constancia de todo ese procedimiento.

## INFORMACIÓN ADICIONAL.

Pueden encontrar más información en la Guía para las fuerzas de seguridad: **https://www.paypalobjects.com/digitalassets/c/website/marketing/na/us/law-enforcement/le-guide-safety-hub.pdf.**

La empresa brinda las siguientes direcciones de correo electrónico a efectos de contactar con sus representantes: **lawenforcement@paypal.com** e **investigaciones@paypal.com.**

# XI. Otros

| ISP | Presevación de información | Entrega voluntariamente IBS | Pedidos de emergencia | Plataforma o correo electrónico |
|---|---|---|---|---|
| **AIRBNB** | - | Sí | Sí | https://airbnb-legal.force.com/ |
| **APPLE** | Sí | Sí | Sí | lawenforcement@apple.com junto con un formulario predeterminado que puede descargarse de: https://www.apple.com/legal/privacy/gle-inforequest-es.pdf |
| **BOOKING** | No | No | Sí | https://www.booking.com/content/law-enforcement-request.es.html |
| **CLOUDFLARE** | Sí | Sí | Sí | abuse+law@cloudflare.com |
| **DISCORD** | Sí | No | Sí | lawenforcement@discord.com |
| **DROPBOX** | Sí | Sí | - | legalcompliance@dropbox.com |
| **EBAY** | - | Sí | - | https://le.corp.ebay.com/ LawEnforcement@ebay.com |
| **ENDURANCE GROUP (INCLUYE PUBLIC DOMAIN REGISTRY)** | Sí | No | - | usdoj@endurance.com |
| **GODADDY** | Sí | No | - | compliancemgr@godaddy.com |
| **GRINDR** | - | Sí | - | legal@grindr.com |
| **HAPPN** | Sí | Sí | Sí | contact@happn.fr support@happn.com |

| | | | | |
|---|---|---|---|---|
| **HORNET** | Sí | No | - | datarequest@hornet.com |
| **HOSTINGER** | Sí | Sí | - | abuse@hostinger.com<br>compliance@hostinger.com |
| **IMPROVMX** | - | Sí | - | support@improvmx.com |
| **LINKEDIN** | Sí | No | Sí | lera_us@linkedin.com<br><br>En el caso de una EMERGENCIA deberá completarse un formulario que puede descargarse de: https://www.linkedin.com/help/linkedin/answer/56372 |
| **MONOVM** | - | Sí | - | abuse@monovm.com |
| **NAMECHEAP** | Sí | No | - | Legal@namecheap.com |
| **NAMESILO** | No | Sí | - | legal@namesilo.com |
| **ONLY FANS** | Sí | Sí | Sí | https://onlyfans.com/legalinquiry |
| **SNAPCHAT** | Sí | Sí | Sí | lawenforcement@snapcht.com<br><br>EMERGENCIAS: https://lawenforcement.snapchat.com/es/emergency |
| **TELEGRAM** | No | No | No | |
| **WORDPRESS** | Sí | NO | - | legal@wordpress.com |
| **YOPMAIL** | Sí | Sí | - | fred.yopmail@gmail.com |
| **ZOOM** | Sí | Sí | Sí | https://zoom.us/trust-form/?enter=Law%20Enforcement%20Request |

REUNIÓN ESPECIALIZADA DE
**MINISTERIOS PÚBLICOS** DEL
MERCOSUR

www.rempm.org