2020

Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia
DIGCRI | Dirección General de Cooperación Regional e Internacional

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

2020

Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia
DIGCRI | Dirección General de Cooperación Regional e Internacional

2020
Guía de Buenas Prácticas para obtener Evidencia Electrónica en el Extranjero

---

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia
DIGCRI | Dirección General de Cooperación Regional e Internacional

---

Diseño: Dirección de Comunicación Institucional
Ministerio Público Fiscal de la Nación.

Índice

PRESENTACIÓN

El objetivo de este documento es brindar a las y los investigadores una herramienta que sirva de guía en caso de que necesiten obtener información electrónica almacenada en el extranjero.

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

Resulta importante destacar que tanto Argentina como los Estados Unidos de América son Estados partes del Convenio sobre Ciberdelito del Consejo de Europa (ETS N° 185), también conocida como Convención de Budapest, por haber sido firmada en esa ciudad el 23 de noviembre de 2001. La República Argentina adhirió a dicho instrumento internacional por ley Nº 27.411, sancionada el 22 de noviembre de 2017, su ratificación se llevó a cabo el 5 de junio de 2018 y, el 1 de octubre de 2018, entró en vigor.

Las recomendaciones sistematizadas en este material fueron elaboradas conjuntamente por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y la Dirección General de Cooperación Regional e Internacional (DIGCRI) del Ministerio Público Fiscal de la Nación sobre la base de documentos oficiales y la experiencia adquirida a lo largo de estos años de trabajo.

I. 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 la legislación de los Estados Unidos de América (EUA) que clasifica 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[1] desde la que se creó la cuenta.

1. La dirección IP identifica una conexión a internet desde un dispositivo (computadora de escritorio o portátil, celular, tableta o cualquier otro equipo con conexión a internet -televisores inteligentes, heladeras u otros dispositivos hogareños comprendidos en lo que se denomina "internet de las cosas"-) en un momento determinado. Esas direcciones IP, que son únicas a través de toda la red de redes, están formadas por un grupo de cuatro segmentos (ej. 200.55.243.205, el número mínimo es 0.0.0.0. y el máximo 255.255.255.255.), se encuentran distribuidas mundialmente en bloques y son asignadas a los clientes por proveedores del servicio de internet –ISP- (ejemplos de ISP en nuestro país son "Fibertel" –de Telecom Argentina S.A., "Speedy" –de Telefónica de Argentina S.A.- e "IPlan" –de NSS S.A.-). En la actualidad este protocolo de direcciones IP, denominado IPv4 está siendo reemplazado por uno nuevo, denominado IPv6 ya que el límite en el número de direcciones de red admisibles en el protocolo IPv4 está empezando a restringir la expansión de Internet y su uso. El nuevo protocolo admite direcciones IP más extensas, las que se presentan mediante caracteres alfanuméricos -sistema hexadecimal-, de forma tal que cada vez más dispositivos conectados a internet podrán tener una dirección IP asignada en forma exclusiva.

- 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 cuenta[2].

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 internacional**. 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 argentinas, será necesario enviar una solicitud de asistencia jurídica para que un juez de Estados Unidos emita una orden en ese sentido.

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).

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.

b. Información transaccional, que incluye usualmente:

- Datos de remitente y receptor de correos electrónicos y sus direcciones IP de conexión.
- Día y hora de las comunicaciones que se efectuaron.
- Cantidad de datos que insumió la comunicación.
- Sitios web visitados por el usuario.

En estos casos, el estándar impone mayores exigencias. Se van a requerir detalles específicos acerca de cómo los registros son relevantes para la investigación. Y la información sólo será entregada si media una orden de un juez local, para lo cual será necesario enviar una **solicitud de asistencia jurídica internacional**[4]**.**

c. Información de contenido, que incluye usualmente:

- 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[5].
- Contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general[6].
- 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**[7] (exhorto internacional).

---

4. Disponible en: https://www.fiscales.gob.ar/wp-content/uploads/2019/12/Gu%C3%ADa-Cooperación-Internacional-MPFN.pdf
5. 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.
6. Por ejemplo, publicaciones en cuentas privadas de Twitter o biografías de grupos cerrados de Facebook.
7. Disponible en: https://www.fiscales.gob.ar/wp-content/uploads/2019/12/Gu%C3%ADa-Cooperación-Internacional-MPFN.pdf

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 de aclaración del uso legítimo de datos en el extranjero**[8] *(Clarifying Lawful Overseas Use of Data Act or CLOUD Act)*, una ley federal de los Estados Unidos -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 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.

Los Tratados[9] vigentes sobre asistencia jurídica en materia penal podrán verse en el siguiente sitio web: http://www.mpf.gob.ar/cooperacion-ai/normativa/

Mientras que desde la intranet del MPF se puede acceder a un modelo de solicitud de asistencia jurídica a los efectos de requerir evidencia electrónica: https://intranet.mpf.gov.ar/cooperacion-internacional/

8. Conf. Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) de fecha 6 de febrero de 2018, disponible en: https://www.congress.gov/bill/115th-congress/house-bill/4943/text, que la CLOUD Act modifica el Stored Communications Act (SCA) of 1986.

9. Nuestro país ha suscripto distintos tratados bilaterales, regionales y multilaterales sobre cooperación internacional con otros Estados, a saber:
Los tratados bilaterales vigentes son: Australia (Ley 24.038), Canadá (Ley 25.460), Colombia (Ley 25.348), China (Ley 26.882), Corea (Ley 26.782), El Salvador (Ley 25.911), España (Ley 23.708), Estados Unidos (Ley 24.034), Francia (Ley 26.196), Italia (Ley 23.707), México (Ley 26.137), Perú (Ley 25.307), Portugal (Ley 26.440), Reino Unido (Ley 3.043), Suiza (Ley 26.781), Túnez (Ley 26.611), Rusia (Ley 27.405), Sudáfrica (Ley 27.018).
Los tratados regionales vigentes para la Argentina son: el Protocolo de Asistencia Jurídica Mutua en Asuntos Penales del MERCOSUR (Ley 25.095), Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales del MERCOSUR, Bolivia y Chile (ley 26.004), y Convención Interamericana sobre Asistencia Mutua en Materia Penal (Ley 26.139).
Los tratados multilaterales vigentes son: Convenio sobre Ciberdelito (Ley 27.411) y Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Ley 25.632).
Para más información se puede consultar el micrositio web de la Dirección Regional de Cooperación Regional e Internacional: https://www.mpf.gob.ar/cooperacion-ai/normativa/

II. 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).

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.

La medida resultaría admisible, a nivel local, en función del principio de libertad probatoria, aunque a partir de la entrada en vigor 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[10].

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

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

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

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.

III. 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).

Cualquier fiscal puede solicitar estas medidas. La UFECI se encuentra a disposición para concretarla o para evacuar cualquier consulta en relación a las firmas con las que se suele trabajar frecuentemente (Facebook, Instagram, WhatsApp, Twitter, Zoom, Netflix, etc.) o a fin de contactar a empresas (en particular, en el extranjero) para establecer cómo realizar una preservación.

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.

Cuando no sea posible contactar a la empresa de la que se trate para preservar registros, dependiendo del territorio en el que se encuentre la empresa o la información que se pretende resguardar, 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.

En nuestro país, al punto de contacto de la red es la **UNIDAD 24/7 de DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL**[11] que funciona en el ámbito de la Dirección Nacional de Asuntos Internacionales del Ministerio de Justicia y Derechos Humanos de la Nación. Esa oficina tiene el objetivo de contribuir a:

- aumentar la eficacia operativa y funcional de la Red 24/7,

- facilitar los mecanismos de comunicación entre la autoridad central encargada de la tramitación de las solicitudes de cooperación internacional, los operadores del sistema penal federal y provinciales y la Red 24/7,

- la cooperación entre la Red 24/7 y los miembros de las redes de otros países.

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[12].

La DIGCRI ha desarrollado guías[13], formularios[14] y ha incorporado, en su micrositio web institucional,

---

11. Conf. Resolución N° 1291/2019 de fecha 25 de noviembre de 2019.

12. La Resolución PGN N° 106/2018 de fecha 11 de octubre de 2018 protocolizó el Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos y Fiscales miembros de la AIAMP suscripto el 6 de septiembre de 2018; y, designó como punto de contacto a la Dirección General de Cooperación Regional e Internacional (DIGCRI).

13. Guía de Cooperación Internacional del Ministerio Público Fiscal de la Nación Argentina disponible en https://www.mpf.gob.ar/cooperacionjuridica/files/2019/12/Gu%C3%ADa-Cooperación-Internacional-MPFN.pdf

14. Disponible en https://intranet.mpf.gov.ar/cooperacion-internacional/pedidos-de-cooperacion-interinstitucional/

los diferentes convenios de cooperación interinstitucional directa vigentes[15] y la guía de uso del Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos y Fiscales Miembros de AIAMP[16].

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

La red 24/7 de crímenes de alta tecnología del G7[17] **(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).

En Argentina, el punto de contacto de esta red es el titular de la UFECI, fiscal Horacio Azzolin.

Para concretar la medida deberá llenarse un formulario (al que se accede desde aquí: http://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/), que deberá ser firmado por juez o fiscal del caso y luego enviado a la casilla de correo: cibercrimen@mpf.gov.ar.

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.

15. Disponible en https://www.mpf.gob.ar/cooperacionjuridica/tipo_de_recurso/acuerdos-interinstitucionales/

16. Disponible en https://www.mpf.gob.ar/cooperacionjuridica/files/2019/11/Gu%C3%ADa-de-Uso-del-Acuerdo-de-Cooperación-Interinstitucional-entre-los-Ministerios-Públicos-y-Fiscales-Miembros-de-la-AIAMP.pdf

17. 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.

IV. 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. También **puede utilizarse alguna de las redes ya citadas p**ara efectuar la solicitud.

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

En cualquier caso, como se trata de casos de urgencia, sugerimos contactar inmediatamente con la UFECI a efectos de poder brindarles la mejor asistencia posible para concretar la medida exitosamente.

V. CONTACTOS

Para información sobre obtención y preservación de evidencia digital comunicarse con:
Unidad Fiscal Especializada en Ciberdelincuencia (UFECI): ufeci@mpf.gov.ar

Para información sobre solicitudes de asistencia jurídica internacional y cooperación interinstitucional comunicarse con **Dirección General de Cooperación Regional e Internacional**: internacional@mpf.gov.ar

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO FISCAL | PROCURACIÓN GENERAL DE LA NACIÓN
Av. de Mayo 760 (C1084AAP) - Ciudad Autónoma de Buenos Aires - Argentina
(54-11) 4338-4300
www.mpf.gob.ar | www.fiscales.gob.ar