



Lineamientos del proceso legal

Agencias gubernamentales y organismos de orden público fuera de Estados Unidos

Las agencias gubernamentales y los organismos de orden público fuera de Estados Unidos deben usar estos lineamientos cuando solicitan información sobre clientes con dispositivos, productos y servicios de Apple a entidades de Apple en la región o el país pertinente. Apple actualizará estos lineamientos cuando sea necesario.

En estos lineamientos, Apple hace referencia a la entidad pertinente que es responsable de la información de los clientes en una región o un país en particular. Como empresa global, Apple tiene varias entidades legales en distintas jurisdicciones que son responsables de la información personal que recopilan y que se procesa en nombre de Apple Inc. Por ejemplo, la información de puntos de venta en sus entidades minoristas fuera de Estados Unidos es controlada por las entidades minoristas individuales de Apple en cada país. Es posible que las entidades legales fuera de Estados Unidos también controlen la información personal relacionada con apple.com y los Servicios de contenido multimedia de Apple, según se detalla en los términos de cada servicio en una jurisdicción específica. En general, las entidades legales de Apple fuera de Estados Unidos en Australia, Canadá, Irlanda y Japón son responsables de los datos de los clientes relacionados con los servicios de Apple en sus respectivas regiones.

Todas las otras solicitudes de información con respecto a clientes de Apple, incluidas las preguntas de clientes sobre la divulgación de información, deben dirigirse a www.apple.com/la/privacy/contact/. Estos lineamientos no se aplican a las solicitudes que las agencias gubernamentales y los organismos de orden público de Estados Unidos realizan a Apple Inc.

Para las solicitudes de información de agencias gubernamentales y organismos de orden público, Apple cumple con las leyes sobre entidades globales que controlan nuestros datos y proporciona detalles cuando la ley así lo requiera. Todas las solicitudes de agencias gubernamentales y organismos de orden público fuera de Estados Unidos sobre contenido, a excepción de circunstancias de emergencia (se definen a continuación en Solicitudes de emergencia), deben cumplir con las leyes aplicables, incluida la Ley de Privacidad para las Comunicaciones Electrónicas (ECPA) de Estados Unidos. Una solicitud conforme a un Tratado de asistencia legal mutua o un Acuerdo ejecutivo en virtud de la Ley Aclaratoria del Uso Legal de Datos en el Extranjero ("Acuerdo de la Ley CLOUD") cumple con la ECPA. Apple proporcionará contenido del cliente como se encuentra en la cuenta del cliente solo como respuesta a dicho proceso legalmente válido.

Para las solicitudes de entidades privadas, Apple cumple con las leyes relativas a las entidades locales que controlan los datos de los clientes y proporciona datos cuando la ley así lo requiere.

Apple tiene un proceso centralizado para recibir, dar seguimiento, procesar y responder las solicitudes legales legítimas de agencias gubernamentales, organismos de orden público y entidades privadas a partir de que se reciben hasta que se proporciona una respuesta. Un equipo capacitado de nuestro

Departamento Legal revisa y evalúa todas las solicitudes que se reciben, y las solicitudes que Apple determina que no tienen fundamentos jurídicos válidos o considera que son ambiguas, inadecuadas o imprecisas se objetan, refutan o rechazan.

Apple proporciona respuestas al organismo de orden público solicitante en la dirección de correo electrónico oficial del oficial solicitante del organismo de orden público. Toda la preservación de las pruebas de conformidad con las respuestas proporcionadas por Apple es responsabilidad del organismo de orden público solicitante.

ÍNDICE

I. Información general

II. Solicitudes legales realizadas a Apple

- A. Solicitudes de información de agencias gubernamentales y organismos de orden público
- B. Administración y respuesta de las solicitudes de información de agencias gubernamentales y organismos de orden público
- C. Solicitudes de preservación
- D. Solicitudes de emergencia
- E. Solicitudes de restricción o eliminación de cuentas
- F. Aviso a los clientes

III. Información disponible de Apple

- A. Registro de dispositivos
- B. Registros del servicio de atención al cliente
- C. Servicios de contenido multimedia de Apple
- D. Transacciones del Apple Store
- E. Pedidos de apple.com
- F. Tarjetas de regalo
- G. Apple Pay
- H. iCloud
- I. Encontrar
- J. AirTag y programa de accesorios de la red de la app Encontrar
- K. Extracción de datos de dispositivos iOS bloqueados con un código
- L. Solicitud de dirección IP
- M. Otra información disponible del dispositivo
- N. Solicitudes de datos del circuito cerrado de televisión (CCTV) del Apple Store
- O. Game Center
- P. Activación de dispositivos iOS
- Q. Registros de conexión
- R. Registros de Mi Apple ID y iForgot
- S. FaceTime
- T. iMessage
- U. App Apple TV
- V. Iniciar sesión con Apple

IV. Preguntas frecuentes

I. Información general

Apple diseña, fabrica y comercializa dispositivos multimedia y de comunicación móvil, computadoras personales y reproductores portátiles de música digital, y vende una variedad de servicios, software, periféricos y soluciones de red relacionados, así como apps y contenido digital de terceros. Los productos y los servicios de Apple incluyen la Mac, el iPhone, el iPad, el iPod touch, el Apple TV, el Apple TV+, el Apple Watch, el HomePod, los AirPods, el AirTag, un conjunto de apps de software profesionales y de consumo, los sistemas operativos iOS y macOS X, iCloud y una variedad de ofertas de soporte, servicio y accesorios. Apple también vende y ofrece contenido digital y apps a través de Apple Music, App Store, Apple Books y Mac App Store. Apple guarda la información de los clientes de acuerdo con la [política de privacidad](#) de Apple y las [condiciones de servicio](#) correspondientes de la oferta de servicio en particular. Apple se compromete a proteger la privacidad de los clientes de los productos y servicios de Apple ("clientes de Apple"). Por lo tanto, excepto en situaciones de emergencia establecidas por la ley, no se revelará información de los clientes de Apple sin un proceso legal válido.

La información que se incluye en estos lineamientos se elaboró para brindar información a agencias gubernamentales y organismos de orden público fuera de Estados Unidos sobre el proceso legal que Apple necesita para divulgar información electrónica a agencias gubernamentales y organismos de orden público fuera de Estados Unidos. El objetivo de estos lineamientos no es brindar asesoramiento legal. El objetivo de la sección Preguntas frecuentes ("FAQ") de estos lineamientos es proporcionar las respuestas a algunas de las preguntas más frecuentes que Apple recibe. Ni estos lineamientos ni las FAQ abordarán cada posible situación que pueda surgir.

Si tienes más preguntas, envía un correo electrónico a lawenforcement@apple.com.

Solo el personal de agencias gubernamentales y organismos de orden público puede usar el buzón de correo anterior. Si elige enviar un correo electrónico a este buzón de correo, debe hacerlo desde una dirección de correo electrónico válida y oficial de una agencia gubernamental o un organismo de orden público.

Las solicitudes legales enviadas a Apple deben solicitar información sobre un dispositivo Apple o cliente en particular y los servicios específicos que Apple puede brindar a ese cliente. Apple puede proporcionar información sobre un dispositivo Apple o cliente siempre y cuando aún tenga la información solicitada conforme a sus políticas de retención de datos. Apple guarda los datos como se especifica en algunas secciones de "Información disponible" a continuación. Todos los otros datos se guardan durante el periodo necesario para alcanzar los objetivos que se especifican en nuestra [política de privacidad](#). Las agencias gubernamentales y los organismos de orden público deben ser lo más precisos y específicos que puedan cuando realizan las solicitudes para evitar interpretaciones erróneas, objeciones, refutaciones o rechazos como respuesta a una solicitud ambigua, inadecuada o imprecisa. Todas las solicitudes de agencias gubernamentales y organismos de orden público fuera de Estados Unidos sobre contenido, a excepción de circunstancias de emergencia (se definen a continuación en Solicitudes de emergencia), deben cumplir con las leyes aplicables, incluida la Ley de Privacidad para las Comunicaciones Electrónicas (ECPA) de Estados Unidos. Una solicitud conforme a un Tratado de asistencia legal mutua o un Acuerdo ejecutivo en virtud de la Ley Aclaratoria del Uso Legal de Datos en el Extranjero ("Acuerdo de la Ley CLOUD") cumple con la ECPA. Apple proporcionará contenido del cliente como se encuentra en la cuenta del cliente solo como respuesta a dicho proceso legalmente válido.

Nada de lo que figura en estos lineamientos tiene como objetivo establecer derechos exigibles contra Apple, y las políticas de Apple se pueden actualizar o cambiar en el futuro sin previo aviso a las agencias gubernamentales o los organismos de orden público.

II. Solicitudes legales realizadas a Apple

A. Solicitudes de información de agencias gubernamentales y organismos de orden público

Apple acepta solicitudes de información de agencias gubernamentales u organismos de orden público legalmente válidas por correo electrónico, siempre y cuando se envíen desde la dirección de correo electrónico oficial de la agencia gubernamental o el organismo de orden público que presenta la solicitud. El personal de agencias gubernamentales y organismos de orden público fuera de Estados Unidos que envía una solicitud de información a Apple debe completar una [plantilla de solicitud de información de agencias gubernamentales y organismos de orden público](#) y enviarla directamente desde la dirección de correo electrónico oficial de la agencia gubernamental o el organismo de orden público a lawenforcement@apple.com.

Solo el personal de agencias gubernamentales y organismos de orden público puede usar el buzón de correo anterior. Cuando las solicitudes tienen cinco identificadores o más, como número de serie del dispositivo/número de identidad internacional de equipo móvil (IMEI), Apple ID, direcciones de correo electrónico o números de factura/pedido, se deben enviar en un formato editable (p. ej., un documento de Numbers, Excel, Pages o Word). Los identificadores como estos generalmente se necesitan para realizar búsquedas de información relacionada con dispositivos, cuentas o transacciones financieras.

Ten en cuenta lo siguiente: Apple no descargará solicitudes legales o documentos relacionados desde ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

Para que Apple pueda divulgar información de clientes como respuesta a la solicitud de un organismo de orden público, es necesario que el oficial que presenta la solicitud indique los fundamentos jurídicos que autorizan que un organismo de orden público obtenga información probatoria en forma de datos personales de parte de un controlador de datos como Apple. Algunos ejemplos de solicitudes que Apple considera legalmente válidas son los siguientes: Production Orders (Australia, Canadá, Nueva Zelanda), lettres de réquisition ou commissions rogatoires (Francia), Solicitud Datos (España), Ordem Judicial (Brasil), Auskunftersuchen (Alemania), Obligation de dépôt (Suiza), 個人情報の開示依頼 (Japón), Personal Data Request, Orders, Warrants and Communications Data Authorisations (Reino Unido), así como órdenes judiciales o solicitudes equivalentes de otros países.

B. Administración y respuesta de las solicitudes de información de agencias gubernamentales y organismos de orden público

Apple revisa con detenimiento todas las solicitudes legales para asegurarse de que haya fundamentos jurídicos válidos para cada solicitud y sean solicitudes legalmente válidas. Si Apple determina que no hay fundamentos jurídicos válidos o si una solicitud es ambigua, inadecuada o imprecisa, Apple objetará, refutará o rechazará la solicitud.

Por motivos de procesamiento y debido a limitaciones del sistema, Apple no puede aceptar solicitudes legales que tengan más de 25 identificadores de cuenta. Si un organismo de orden público presenta solicitudes legales con más de 25 identificadores de cuenta, Apple responderá los primeros 25 y el organismo de orden público tendrá que reenviar una nueva solicitud legal para los identificadores adicionales.

C. Solicitudes de preservación

Todas las solicitudes de agencias gubernamentales y organismos de orden público fuera de Estados Unidos sobre contenido, a excepción de circunstancias de emergencia (se definen a continuación en Solicitudes de emergencia), deben cumplir con las leyes aplicables, incluida la Ley de Privacidad para las Comunicaciones Electrónicas (ECPA) de Estados Unidos. A una solicitud conforme un Tratado de asistencia legal mutua o un Acuerdo ejecutivo en virtud de la Ley Aclaratoria del Uso Legal de Datos en el Extranjero ("Acuerdo de la Ley CLOUD") cumple con la ECPA. Deberá enviarse una solicitud de preservación de la información con anterioridad a la inminente solicitud conforme a la ECPA por correo electrónico a lawenforcement@apple.com.

Las solicitudes de preservación deben incluir la dirección de correo electrónico de la cuenta o el Apple ID pertinente, o bien el nombre completo y el número de teléfono, o el nombre completo y la dirección física del cliente de la cuenta de Apple. Cuando se reciba una solicitud de preservación, Apple preservará la extracción de datos por única vez de los datos existentes del cliente que se hayan solicitado y que estén disponibles al momento de la solicitud durante 90 días. Después de este periodo de 90 días, se eliminará automáticamente la preservación del servidor de almacenamiento. Sin embargo, este periodo se puede ampliar a un periodo adicional de 90 días si se presenta una nueva solicitud. Si se intenta presentar más de dos solicitudes de preservación para la misma cuenta, la segunda solicitud se tratará como una solicitud de ampliación de la preservación original y no como una preservación independiente de datos nuevos.

D. Solicitudes de emergencia

Apple considera que una solicitud es una solicitud de emergencia cuando está relacionada con circunstancias que implican amenazas inminentes y graves para la vida/seguridad de las personas, la seguridad de un estado o la seguridad de infraestructuras/instalaciones esenciales.

Si el oficial de la agencia gubernamental o el organismo de orden público que realiza la solicitud confirman satisfactoriamente que la solicitud está relacionada con circunstancias de emergencia que implican uno o más de los criterios anteriores, Apple examinará dicha solicitud con carácter de urgente.

Para solicitar que Apple divulgue información voluntariamente con carácter de urgente, el oficial de la agencia gubernamental o el organismo de orden público que presenta la solicitud debe completar el [formulario de solicitud de emergencia de información de agencias gubernamentales y organismos de orden público](#) y enviarlo directamente desde la dirección de correo electrónico oficial de la agencia gubernamental o el organismo de orden público a exigent@apple.com con las palabras "Emergency Request" (Solicitud de emergencia) en el asunto.

Si una agencia gubernamental o un organismo de orden público solicita datos de clientes como respuesta a una solicitud de emergencia de información de agencias gubernamentales y organismos de orden público, se puede llamar a un supervisor del agente de la agencia gubernamental o el organismo de orden público que envió la solicitud de emergencia de información de agencias gubernamentales y organismos de orden público y pedirle que confirme a Apple que la solicitud de emergencia es legítima. El agente de la agencia gubernamental o el organismo de orden público que envió la solicitud de emergencia de información de agencias gubernamentales y organismos de orden público deben proporcionar la información de contacto del supervisor en la solicitud.

Si una agencia gubernamental o un organismo de orden público necesita comunicarse con Apple por una consulta urgente, comuníquese con el Global Security Operations Center (GSOC) de Apple llamando al 001 408 974-2095. Este número de teléfono ofrece servicio en varios idiomas.

E. Solicitudes de restricción o eliminación de cuentas

Si una agencia gubernamental o un organismo de orden público solicita que Apple restrinja o elimine el Apple ID de un cliente, Apple necesitará una orden judicial o un proceso legal equivalente en el país en cuestión (a menudo una condena o una orden judicial) que demuestre que la cuenta que se solicita restringir o eliminar se usó de manera ilícita.

Apple revisa con detenimiento todas las solicitudes de agencias gubernamentales y organismos de orden público para asegurarse de que haya fundamentos jurídicos válidos para cada solicitud. En los casos en que Apple determine que no existe una base legal válida o si la orden judicial no demuestra que la cuenta que se restringirá/eliminará se usó de manera ilegal, Apple rechazará/impugnará la solicitud.

Cuando Apple reciba una orden judicial válida u otro proceso legal equivalente en el país en cuestión (a menudo una condena o una orden judicial) de una agencia gubernamental o un organismo de orden público que demuestre que la cuenta que se solicita restringir o eliminar se usó de manera ilícita, Apple tomará las medidas necesarias para restringir o eliminar la cuenta conforme a la orden judicial y asesorará al agente que lo solicita según corresponda.

F. Aviso a los clientes

Apple notificará a los clientes cuando se solicite información de su cuenta de Apple como respuesta a una solicitud legalmente válida de una agencia gubernamental o un organismo de orden público, a excepción de los siguientes casos: cuando la solicitud legalmente válida, una orden judicial que Apple recibe o las leyes aplicables prohíban explícitamente enviar un aviso; cuando Apple, a su entera discreción, crea que enviar dicho aviso puede representar un riesgo de lesión o muerte para una persona concreta; en situaciones en las que el caso se relacione con un peligro para un niño; o cuando el aviso no corresponda a los hechos subyacentes del caso.

Después de 90 días, Apple aplazará el aviso para las divulgaciones de emergencia, a excepción de los siguientes casos: cuando una orden judicial o las leyes aplicables prohíban enviar un aviso; cuando Apple, a su entera discreción, crea que dicho aviso puede representar un riesgo de lesión o muerte para una persona concreta o un grupo de personas; o en situaciones en las que el caso se relacione con un peligro para un niño. Apple aplazará el aviso después de que se cumpla el periodo de no divulgación que se especifica en una orden judicial, a menos que Apple, a su entera discreción, crea razonablemente que enviar dicho aviso puede representar un riesgo de lesión o muerte para una persona concreta o un grupo de personas, el caso se relacione con un peligro para un niño o el aviso no corresponda a los hechos subyacentes del caso.

Apple notificará a los clientes cuando su cuenta de Apple se haya restringido o eliminado como consecuencia de haber recibido una orden judicial (a menudo una condena o una orden judicial) que demuestre que la cuenta que se solicita restringir o eliminar se usó de manera ilícita o infringió las condiciones de servicio de Apple, a excepción de los siguientes casos: cuando el proceso legal, una orden judicial que Apple recibe o las leyes aplicables prohíban enviar un aviso; en situaciones en las que el caso se relacione con un peligro para un niño; cuando Apple, a su entera discreción, crea razonablemente que enviar dicho aviso puede representar un riesgo de lesión o muerte para una

persona concreta o un grupo de personas; o cuando el aviso no corresponda a los hechos subyacentes del caso.

III. Información disponible de Apple

En esta sección, se abordan los tipos generales de información que puede proporcionar Apple al momento de la publicación de estos lineamientos.

A. Registro de dispositivos

Los clientes proporcionan a Apple información básica de registro o del cliente, incluido el nombre, la dirección, la dirección de correo electrónico y el número de teléfono, cuando registran un dispositivo Apple anterior a iOS 8 y macOS Sierra 10.12. Apple no verifica esta información, y es posible que no sea precisa ni refleje al propietario del dispositivo. La información de registro de los dispositivos con iOS 8 y versiones posteriores, y las Mac con macOS Sierra 10.12 y versiones posteriores se recibe cuando un cliente asocia un dispositivo con un Apple ID de iCloud. Es posible que esta información no sea precisa ni detalle quién es el propietario del dispositivo. La información de registro, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del solicitante.

Ten en cuenta que los números de serie de los dispositivos Apple no incluyen las letras "O" ni "I". Apple usa los números 0 (cero) y 1 (uno) en los números de serie. Las solicitudes de números de serie con las letras "O" o "I" no tendrán resultados. Cuando una solicitud legal tiene cinco números de serie o más, Apple solicita que también se envíen estos números de serie en formato electrónico editable (p. ej., un documento de Numbers, Excel, Pages o Word).

B. Registros del servicio de atención al cliente

Se puede obtener información de Apple sobre las comunicaciones que los clientes tuvieron con el servicio de atención al cliente de Apple con respecto a un dispositivo o servicio. Esta información puede incluir registros de interacciones de soporte técnico con los clientes respecto de un dispositivo o servicio de Apple en particular. Además, es posible que también esté disponible la información del dispositivo, la garantía y la reparación. Esta información, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del solicitante.

C. Servicios de contenido multimedia de Apple

App Store, Apple Music, la app Apple TV, Apple Podcasts y Apple Books ("Servicios de contenido multimedia de Apple") son apps de software que los clientes usan para organizar y reproducir apps, música y videos digitales, y para transmitir contenido. Los Servicios de contenido multimedia de Apple también proporcionan contenido para que los clientes descarguen en sus computadoras y dispositivos iOS. Cuando un cliente abre una cuenta de Apple, puede proporcionar información básica suya, como nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, es posible que también esté disponible información sobre conexiones y transacciones de compra o descarga de los Servicios de contenido multimedia de Apple y conexiones para obtener actualizaciones o volver a realizar descargas. Es posible que la información de las direcciones IP se limite a los 18 meses más recientes. Se pueden obtener información de los clientes de los Servicios de

contenido multimedia de Apple y los registros de conexión con direcciones IP, siempre que estos estén disponibles, mediante la correspondiente solicitud legalmente válida del país del solicitante.

Las solicitudes de datos de los Servicios de contenido multimedia de Apple deben incluir el identificador del dispositivo Apple (número de serie, identidad internacional de equipo móvil [IMEI], identificador de equipo móvil [MEID] o identificador único global [GUID]) o la dirección de correo electrónico de la cuenta o el Apple ID pertinente. Si se desconoce la dirección de correo electrónico de la cuenta o el Apple ID, es necesario proporcionarle a Apple la información del cliente de los Servicios de contenido multimedia de Apple, como nombre completo y número de teléfono, o nombre completo y dirección física, para identificar la cuenta del cliente de los Servicios de contenido multimedia de Apple. Es posible que los oficiales de las agencias gubernamentales o los organismos de orden público también proporcionen un número de pedido de los Servicios de contenido multimedia de Apple válido o un número completo de tarjeta de débito o crédito asociado con las compras de los Servicios de contenido multimedia de Apple. Es posible que también se proporcione el nombre de un cliente con estos parámetros, pero el nombre del cliente solo no es suficiente para obtener información.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta de crédito/débito, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encriptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

D. Transacciones del Apple Store

Las transacciones en el punto de venta son transacciones con tarjetas de regalo, tarjetas de crédito/débito o en efectivo que se realizan en un Apple Store. Las solicitudes de registros del punto de venta deben incluir el número completo de la tarjeta de crédito/débito que se usó y también pueden incluir información adicional, como la fecha y hora de la transacción, el monto y los artículos comprados. Se puede obtener información sobre el tipo de tarjeta asociada con una compra en particular, el nombre del comprador, la dirección de correo electrónico, la fecha/hora de la transacción, el monto de la transacción y la ubicación de la tienda, siempre que esta esté disponible, con la correspondiente solicitud legalmente válida del país del solicitante.

Las solicitudes de copias duplicadas de los recibos deben incluir el número de transacción minorista asociado con la compra y, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta de crédito/débito, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encriptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

E. Pedidos de apple.com

Apple tiene información sobre los pedidos realizados en línea en apple.com, la cual puede incluir nombre del comprador, dirección de envío, número de teléfono, dirección de correo electrónico, producto que se compró, monto de la compra y dirección IP de la compra. Las solicitudes de información con respecto a los pedidos realizados en línea en apple.com deben incluir el número completo de la tarjeta de crédito/débito o el número de pedido o el número de serie del artículo que se compró. Es posible que también se proporcione el nombre de un cliente con estos parámetros, pero el nombre del cliente solo no es suficiente para obtener información. Las solicitudes de información relativas a los pedidos realizados en línea en apple.com también pueden incluir la dirección de correo electrónico de la cuenta o el Apple ID pertinente. Si se desconoce la dirección de correo electrónico de la cuenta o el Apple ID, Apple necesitará información del cliente, como nombre completo y número de teléfono, o nombre completo y dirección física, para identificar la cuenta de Apple de la persona. La información sobre las compras realizadas en apple.com, siempre que esté disponible, se puede obtener con una solicitud legalmente válida del país del solicitante.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta de crédito/débito, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encryptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

F. Tarjetas de regalo

Las tarjetas Apple Store y las tarjetas App Store y iTunes tienen un número de serie. Estos números de serie tienen varios formatos que dependen de variables como el diseño o la fecha de emisión. Apple puede proporcionar la información disponible sobre las tarjetas Apple Store, App Store y iTunes como respuesta a la correspondiente solicitud legalmente válida para el país del solicitante. En los casos en que una solicitud legal tiene cinco números de serie de la tarjeta de regalo o más, Apple solicita que se envíen estos números de serie de la tarjeta de regalo en un documento/archivo protegido con contraseña/encryptado (p. ej., un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado.

i. Tarjetas Apple Store

Las tarjetas Apple Store se pueden usar para realizar compras en apple.com o en un Apple Store. Es posible que los registros disponibles incluyan información del comprador de la tarjeta de regalo (si la compró a Apple en lugar de a un comerciante independiente), las transacciones de compra relacionadas y los artículos que se compraron. En algunos casos, Apple puede cancelar o suspender una tarjeta Apple Store según el estado de la tarjeta específica. Se puede obtener información de la tarjeta Apple Store, siempre que esta esté disponible, con la correspondiente solicitud legalmente válida del país del solicitante.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta Apple Store, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encryptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

ii. Tarjetas App Store y iTunes

Las tarjetas App Store y iTunes se pueden usar en Apple Music, App Store, Apple Books y Mac App Store. Con el número de serie, Apple puede determinar si la tarjeta App Store y iTunes se activó (se compró en un punto de venta minorista) o se canjeó (se agregó al saldo del crédito de la tienda de una cuenta de Apple).

Cuando se activa una tarjeta App Store y iTunes, los registros disponibles pueden incluir el nombre de la tienda, la ubicación, la fecha y la hora. Cuando se canjea una tarjeta App Store y iTunes, los registros disponibles pueden incluir la información del cliente de la cuenta de Apple relacionada, la fecha y la hora de activación o canje y la dirección IP del canje. En algunos casos, Apple puede desactivar una tarjeta App Store y iTunes según el estado de la tarjeta específica. Se puede obtener información de la tarjeta App Store y iTunes, siempre que esta esté disponible, con la correspondiente solicitud legalmente válida del país del solicitante.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta App Store y iTunes, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encryptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

G. Apple Pay

Las transacciones de Apple Pay realizadas en locales minoristas (p. ej., para comunicaciones NFC o sin contacto físico) y en apps o puntos de venta en línea se autentican de forma segura en el dispositivo del cliente y se envían encriptadas al comerciante o a su procesador de pagos. Si bien un servidor de Apple verifica la seguridad de las transacciones, Apple no procesa los pagos ni almacena dichas transacciones ni los números de tarjetas de crédito/débito enteros asociados con compras realizadas con Apple Pay. Esta información puede estar disponible a través del banco emisor correspondiente, la red de pagos o el comerciante.

Puede obtener más información sobre los países y las regiones que aceptan Apple Pay en support.apple.com/es-lamr/HT207957.

A fin de solicitar datos transaccionales de las compras realizadas en tiendas Apple Store o mediante apple.com, Apple requiere el número de cuenta principal del dispositivo (DPAN) que se usó para realizar la transacción. El DPAN tiene 16 dígitos y puede obtenerse del banco emisor. Nota: El DPAN se usa en transacciones de pago sin contacto con el comercio en lugar del número de tarjeta de crédito o débito real (FPAN o número de cuenta principal de fondos). El procesador del pago convierte el DPAN en el FPAN correspondiente. Con la información del DPAN correspondiente, Apple puede realizar una búsqueda razonable de información de respuesta a través de su sistema de puntos de venta. Se pueden obtener estos registros, siempre que estos estén disponibles, con la correspondiente solicitud legalmente válida del país del solicitante.

Apple puede proporcionar información de Apple Pay sobre los tipos de tarjetas de crédito/débito que un cliente agregó a Apple Pay junto con información del cliente. Esta información, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del

solicitante. Para solicitar dicha información, Apple requeriría el identificador del dispositivo (número de serie de Apple, SEID, IMEI o MEID) o la dirección de correo electrónico de la cuenta o el Apple ID.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye el DPAN, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encryptado (un archivo PDF y en formato editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

H. iCloud

iCloud es el servicio en la nube de Apple que permite a los clientes acceder a sus fotos, documentos y más desde todos sus dispositivos. iCloud también les permite a los clientes hacer respaldos de sus dispositivos iOS y iPadOS en iCloud. Con el servicio de iCloud, los clientes pueden configurar una cuenta de correo electrónico de iCloud.com. Los dominios de correo electrónico de iCloud pueden ser @icloud.com, @me.com y @mac.com. Todos los datos de contenido de iCloud almacenados por Apple están encryptados en la ubicación del servidor. Para los datos que Apple puede desencriptar, Apple conserva las claves de encryptación en sus centros de datos de Estados Unidos. Apple no recibe ni conserva claves de encryptación para los datos encryptados de un extremo a otro del cliente.

iCloud es un servicio basado en los clientes. Las solicitudes de datos de iCloud deben incluir la dirección de correo electrónico de la cuenta o el Apple ID pertinente. Si se desconoce la dirección de correo electrónico de la cuenta o el Apple ID, Apple necesitará información del cliente, como nombre completo y número de teléfono, o nombre completo y dirección física, para identificar la cuenta de Apple de la persona. Cuando solo se proporcione la dirección de correo electrónico de la cuenta o el Apple ID, se podrá facilitar la información disponible sobre las cuentas verificadas que estén asociadas con estos criterios.

I. Es posible que esté disponible la siguiente información de iCloud:

I. Información del cliente

Cuando los clientes configuran una cuenta de iCloud, es posible que se proporcione a Apple información básica de los clientes, como nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, la información sobre las conexiones de funcionalidades de iCloud también puede estar disponible. La información de los clientes de iCloud y los registros de conexión con las direcciones IP, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante. Los registros de conexión se guardan hasta 25 días.

II. Registros de Mail

Los registros de correo incluyen registros de las comunicaciones entrantes y salientes, como la hora, la fecha, las direcciones de correo electrónico del remitente y las direcciones de correo electrónico del destinatario. Los registros de correo de iCloud se conservan hasta 25 días; y, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

III. Contenido de correo electrónico y otro contenido de iCloud, Secuencia de fotos, Fototeca de iCloud, iCloud Drive, Contactos, Calendarios, Favoritos, Historial de navegación de Safari, Historial de búsqueda de Mapas, Mensajes, Respallos de dispositivos iOS

iCloud almacena contenido de los servicios que el cliente decidió conservar en la cuenta mientras su cuenta permanece activa. Apple no conserva el contenido eliminado una vez que se elimina de los servidores de Apple. El contenido de iCloud puede incluir correos electrónicos, fotos almacenadas, documentos, contactos, calendarios, marcadores, el historial de navegación de Safari, el historial de búsqueda de Mapas, mensajes y respaldos de dispositivos iOS. Los respaldos de los dispositivos iOS pueden incluir fotos y videos en el rollo fotográfico, la configuración del dispositivo, los datos de las apps, los mensajes de iMessage, Business Chat, SMS y MMS y el correo de voz. Todos los datos de contenido de iCloud almacenados por Apple están encriptados en la ubicación del servidor. Para los datos que Apple puede desencriptar, Apple conserva las claves de encriptación en sus centros de datos de Estados Unidos. Apple no recibe ni conserva claves de encriptación para los datos encriptados de un extremo a otro del cliente.

Todas las solicitudes de agencias gubernamentales y organismos de orden público fuera de Estados Unidos sobre contenido, a excepción de circunstancias de emergencia (que se definieron anteriormente en Solicitudes de emergencia), deben cumplir con las leyes aplicables, incluida la Ley de Privacidad para las Comunicaciones Electrónicas (ECPA) de Estados Unidos. Una solicitud conforme a un Tratado de asistencia legal mutua o un Acuerdo ejecutivo en virtud de la Ley Aclaratoria del Uso Legal de Datos en el Extranjero ("Acuerdo de la Ley CLOUD") cumple con la ECPA. Apple proporcionará contenido del cliente como se encuentra en la cuenta del cliente solo como respuesta a dicha solicitud legalmente válida.

II. Protección avanzada de datos

La protección avanzada de datos para iCloud es una funcionalidad que usa encriptación de extremo a extremo para proteger los datos de iCloud con el nivel más alto de seguridad de datos de Apple. Para los usuarios que activan la protección avanzada de datos para iCloud, es posible que haya datos limitados de iCloud disponibles. Puedes encontrar más información sobre la protección avanzada de datos en support.apple.com/es-lamr/guide/security/advanced-data-protection-for-icloud-sec973254c5f/web y support.apple.com/es-lamr/HT212520.

La siguiente información puede estar disponible en iCloud si un usuario activó la protección de datos avanzada para iCloud:

a. Información del cliente

Cuando los clientes configuran una cuenta de iCloud, es posible que se proporcione a Apple información básica de los clientes, como nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, también puede haber información disponible sobre las conexiones de las funcionalidades de iCloud. La información de los clientes de iCloud y los registros de conexión con direcciones IP, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante. Los registros de conexión se guardan hasta 25 días.

b. Registros de correo

Los registros de correo incluyen registros de las comunicaciones entrantes y salientes, como la hora, la fecha, las direcciones de correo electrónico del remitente y las

direcciones de correo electrónico del destinatario. Los registros de correo de iCloud se conservan hasta 25 días; y, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

c. Contenido del correo electrónico y otro contenido de iCloud

En el caso de los usuarios que tienen activada la protección avanzada de datos, iCloud almacena el contenido del correo electrónico, los contactos y los calendarios que los clientes han decidido mantener en la cuenta mientras esta permanece activa. Estos datos se pueden proporcionar, tal como están en la cuenta del cliente, con la correspondiente solicitud legalmente válida del país del solicitante. Apple almacena estos datos limitados y los encripta adicionalmente en la ubicación del servidor. Para los datos que Apple puede desencriptar, Apple conserva las claves de encriptación en sus centros de datos de Estados Unidos. Apple no recibe ni conserva claves de encriptación para los datos encriptados de un extremo a otro del cliente.

La protección de datos avanzada usa la encriptación de un extremo a otro, y Apple no puede desencriptar cierto contenido de iCloud, como Fotos, iCloud Drive, Respaldo, Notas y Marcadores de Safari. En algunas circunstancias, Apple puede retener información limitada relacionada con estos servicios de iCloud, que se puede obtener, siempre que esté disponible, con la correspondiente solicitud legalmente válida del país del solicitante.

III. Retransmisión privada de iCloud

La retransmisión privada de iCloud es un servicio de privacidad de Internet que se ofrece como parte de una suscripción a iCloud+. La retransmisión privada protege la navegación web de los usuarios en Safari, las consultas de resolución de DNS (espacio de nombres de dominio) y el tráfico de las apps http sin encriptar. Los usuarios deben tener una suscripción a iCloud+ y un dispositivo con iOS 15, iPadOS 15 o macOS Monterey (macOS 12) o versiones posteriores para usar la retransmisión privada de iCloud. Puedes encontrar más información sobre la retransmisión privada en support.apple.com/es-lamr/HT212614 y www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

Cuando la retransmisión privada está activada, las solicitudes de navegación web del usuario se envían a través de dos retransmisiones de Internet seguras e independientes. La dirección IP del usuario es visible para el proveedor de red del usuario y para la primera retransmisión, que opera Apple. Los registros DNS del usuario están encriptados, por lo que ninguna de las partes puede ver la dirección del sitio web que el usuario está intentando visitar. La segunda retransmisión, que es operada por un proveedor de contenido externo, genera una dirección IP temporal, desencripta el nombre del sitio web que solicitó el usuario y conecta al usuario con el sitio. La retransmisión privada valida que el cliente que se conecta es un iPhone, un iPad o una Mac. La retransmisión privada reemplaza la dirección IP original del usuario por una asignada del rango de direcciones IP que usa el servicio. La dirección IP de retransmisión asignada se puede compartir entre más de un usuario de la retransmisión privada en la misma área.

Cuando las solicitudes de navegación web del usuario usan la retransmisión privada, Apple no puede determinar la dirección IP del cliente del usuario o la cuenta de usuario correspondiente a partir de las direcciones IP de la retransmisión privada. Apple no tiene información que proporcionar con respecto al Apple ID asociado con la dirección IP de la retransmisión privada.

Nota: La retransmisión privada de iCloud no está disponible en todos los países o regiones. Si los usuarios tienen activada la retransmisión privada y viajan a algún lugar donde no está disponible, se desactivará automáticamente y se volverá a activar cuando los usuarios vuelvan a ingresar a un país o región que la admita.

I. Encontrar

Encontrar es una funcionalidad que activa el usuario mediante la cual un cliente de iCloud puede buscar el iPhone, el iPad, el iPod touch, el Apple Watch, los AirPods, la Mac o el AirTag que perdió o tomar ciertas medidas, como poner el dispositivo en modo perdido, bloquearlo o borrar su contenido. Puedes encontrar más información sobre este servicio en www.apple.com/la/icloud/find-my/.

Para que la funcionalidad Encontrar funcione para un cliente que perdió su dispositivo, el cliente tiene que haberla activado en ese dispositivo específico antes de que se perdiera. La funcionalidad Encontrar de un dispositivo no se puede activar de manera remota ni después de que se perdió el dispositivo o luego de recibir una solicitud de una agencia gubernamental o un organismo de orden público. La información de los servicios de localización del dispositivo se almacena en cada dispositivo individual y Apple no puede recuperar esta información desde un dispositivo específico. La información de los servicios de localización de un dispositivo localizado a través de la funcionalidad Encontrar pertenece al cliente y Apple no tiene el contenido de mapas ni alertas que se transmiten por medio del servicio. En el siguiente enlace de soporte, se brinda información y pasos que el cliente puede seguir si un dispositivo iOS se pierde o fue robado: support.apple.com/es-lamr/HT201472.

Los registros de conexión de Encontrar están disponibles durante un periodo máximo de 25 días y, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante. La actividad transaccional de Encontrar de solicitudes para bloquear o borrar el contenido de un dispositivo de manera remota, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del solicitante.

J. AirTag y programa de accesorios de la red de la app Encontrar

Con la app Encontrar en el iPhone, el iPad, el iPod touch y la Mac, los clientes pueden localizar fácilmente objetos personales si colocan un AirTag o usan un producto que forma parte del programa de accesorios de la red de la app Encontrar.

Con AirTag y iOS 14.5 y macOS 11.3 o versiones posteriores, los clientes pueden recibir ayuda para encontrar artículos personales perdidos (llaves, mochilas, equipaje, etc.) mediante la app Encontrar. El AirTag debe estar dentro del rango de Bluetooth del iPhone, el iPad o el iPod touch enlazado a fin de reproducir un sonido o usar la funcionalidad Rastreo Preciso con modelos de iPhone compatibles. Si el AirTag no se encuentra cerca de su propietario, se puede proporcionar su ubicación aproximada si está dentro del rango de un dispositivo que forma parte de la red de la app Encontrar, la cual está compuesta por cientos de millones de dispositivos Apple de todo el mundo. Puedes encontrar más información en: support.apple.com/es-lamr/HT212227 y support.apple.com/es-lamr/HT210967.

El programa de accesorios de la red de Encontrar les habilita la red de Encontrar a productos de fabricantes de dispositivos terceros (bicicletas, audífonos, etc.) para usar el servicio de modo que los clientes puedan encontrar sus productos de terceros compatibles con la app Encontrar con iOS 14.3 y macOS 11.1 o versiones posteriores.

Para agregar el AirTag o productos de terceros compatibles a la pestaña Artículos de la app Encontrar, los clientes deben tener un Apple ID, haber iniciado sesión en su cuenta de iCloud y habilitado Encontrar, y registrar su AirTag o producto de terceros compatible en su Apple ID. La interacción se encripta de punto a punto, y Apple no puede conocer la ubicación de ningún AirTag o producto de terceros compatible. Puedes obtener más información en support.apple.com/es-lamr/HT211331.

Con un número de serie, es posible que Apple pueda proporcionar los detalles de la cuenta enlazada en respuesta a la correspondiente solicitud legalmente válida del país del solicitante. El historial de enlace del AirTag está disponible durante un periodo de hasta 25 días. En el siguiente enlace de soporte técnico, se brinda información sobre cómo encontrar un número de serie de AirTag: support.apple.com/es-lamr/HT211658.

Ten en cuenta que los números de serie de los dispositivos Apple no incluyen las letras "O" ni "I". Apple usa los números 0 (cero) y 1 (uno) en los números de serie. Las solicitudes de números de serie con las letras "O" o "I" no tendrán resultados. Cuando una solicitud legal tiene cinco números de serie o más, Apple solicita que también se envíen estos números de serie en formato electrónico editable (p. ej., un documento de Numbers, Excel, Pages o Word).

K. Extracción de datos de dispositivos iOS bloqueados con un código

Para todos los dispositivos con iOS 8.0 y versiones posteriores, Apple no puede realizar una extracción de datos del dispositivo iOS, ya que los datos que generalmente solicitan los organismos de orden público están encriptados y Apple no tiene la clave de encriptación. Todos los iPhone 6 y modelos posteriores se fabrican con iOS 8.0 o una versión posterior de iOS.

Para los dispositivos con iOS 4, 5, 6 y 7, Apple puede, según el estado del dispositivo, realizar extracciones de datos de iOS conforme a la Ley de Privacidad para las Comunicaciones Electrónicas de California (CalECPA, secciones 1546-1546.4 del Código Penal de California). Para que Apple realice una extracción de datos de iOS en un dispositivo que cumple con estos criterios, las autoridades del orden público deben obtener una orden de registro emitida tras demostrar una causa probable según la CalECPA. Además de la CalECPA, Apple no identificó ninguna autoridad legal establecida que requiera que Apple extraiga datos como tercero en una investigación judicial.

L. Solicitud de dirección IP

Antes de enviar un proceso legal con una dirección IP como identificador, Apple solicita que las autoridades del orden público determinen que la dirección IP del sujeto no es una dirección IP pública o del enrutador y que no usa la traducción de direcciones de red de nivel de operador (CGNAT). Además, solicita que le confirmen que es una dirección IP privada durante el servicio del proceso legal. Además, dichas solicitudes deben incluir una restricción de fecha de no más de tres días. En respuesta a dicha solicitud, Apple puede producir registros de conexión (ver la sección III.Q a continuación) a partir de los cuales las autoridades del orden público pueden intentar identificar una cuenta de Apple/Apple ID en particular para usar como identificador en una solicitud de seguimiento de un proceso legal. Los datos de los clientes de Apple basados en una dirección IP, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

M. Otra información disponible del dispositivo

Dirección MAC: Una dirección de control de acceso al medio (dirección MAC) es un identificador único que se asigna a interfaces de red para comunicaciones en un segmento de red físico. Cualquier producto Apple con interfaces de red tendrá una o más direcciones MAC, como Bluetooth, Ethernet, Wi-Fi o FireWire. Al proporcionar a Apple un número de serie (o, en el caso de un dispositivo iOS, un IMEI, MEID o UDID), se puede obtener información pertinente sobre la dirección MAC, siempre que esté disponible, con la correspondiente solicitud legalmente válida del país del solicitante.

N. Solicitudes de datos del circuito cerrado de televisión (CCTV) del Apple Store

Los datos del CCTV pueden variar según la ubicación de la tienda. Los datos del CCTV generalmente se guardan en un Apple Store durante un periodo máximo de 30 días. En varias jurisdicciones, se guardan solo veinticuatro (24) horas conforme a las leyes locales. Después de que transcurre este periodo, es posible que los datos no estén disponibles. Se pueden enviar las solicitudes que son solo para datos del CCTV a lawenforcement@apple.com. La agencia gubernamental o el organismo de orden público deben proporcionar la fecha, la hora y la información de la transacción relacionada con respecto a los datos solicitados.

O. Game Center

Game Center es una red social de juegos de Apple. La información sobre las conexiones de Game Center de un cliente o un dispositivo puede estar disponible. Los registros de conexión, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

P. Activación de dispositivos iOS

Cuando un cliente activa un dispositivo iOS con un proveedor de servicio celular o actualiza el software, el proveedor de servicio o el dispositivo proporcionan a Apple determinada información según el evento. Las direcciones IP del evento, los números del identificador de la tarjeta del circuito integrado (ICCID) y otros identificadores del dispositivo pueden estar disponibles. Esta información, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del solicitante.

Doble SIM: En el caso de los dispositivos con doble SIM, la información del operador con respecto a la nano SIM o eSIM, siempre que esté disponible, se puede obtener con la correspondiente solicitud legalmente válida del país del solicitante. Una eSIM es una tarjeta SIM digital que les permite a los clientes activar un plan de datos celulares de un operador sin tener que usar una nano-SIM física. Puedes obtener más información en support.apple.com/es-lamr/HT209044. En China continental, Hong Kong y Macao, el iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max y iPhone XR tienen doble SIM con dos tarjetas nano-SIM.

Q. Registros de conexión

La actividad de conexión de un cliente o un dispositivo a servicios de Apple como Apple Music, la app Apple TV, Apple Podcasts, Apple Books, iCloud, Mi Apple ID y Apple Discussions, siempre que esté disponible, se puede obtener de Apple. Estos registros de conexión con las direcciones IP, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

R. Registros de Mi Apple ID y iForgot

Se pueden obtener los registros de Mi Apple ID y iForgot que tiene Apple sobre un cliente. Es posible que los registros de Mi Apple ID y iForgot incluyan información sobre las medidas para restablecer la contraseña. Los registros de conexión con las direcciones IP, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

S. FaceTime

Las comunicaciones de FaceTime están encriptadas completamente y Apple no tiene forma de descryptar los datos de FaceTime cuando están en tránsito entre dispositivos. Apple no puede interceptar las comunicaciones de FaceTime. Apple tiene registros de invitaciones de llamadas de FaceTime cuando se inicia una invitación de llamada de FaceTime. En estos registros, no se indica que en realidad existió una comunicación entre los clientes. Los registros de invitaciones de llamadas de FaceTime se guardan hasta 25 días. Los registros de invitaciones de llamadas de FaceTime, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

T. iMessage

Las comunicaciones de iMessage están encriptadas completamente y Apple no tiene forma de descryptar los datos de iMessage cuando están en tránsito entre dispositivos. Apple no puede interceptar las comunicaciones de iMessage ni tiene los registros de las comunicaciones de iMessage. Apple tiene los registros de consultas sobre la capacidad de iMessage. En estos registros, se indica que una app del dispositivo (puede ser Mensajes, Contactos, Teléfono u otra app del dispositivo) inició una consulta y la redirigió a los servidores de Apple para que un controlador de búsqueda (puede ser un número de teléfono, una dirección de correo electrónico o un Apple ID) determine si ese controlador de búsqueda “admite iMessage”. Los registros de consultas de la capacidad de iMessage no indican que realmente se haya realizado alguna comunicación entre los clientes. Apple no puede determinar si en realidad existió una comunicación de iMessage en función de los registros de consultas sobre la capacidad de iMessage. Apple tampoco puede identificar la app real que inició la consulta. Los registros de consultas de la capacidad de iMessage no confirman que realmente se intentó un evento de iMessage. Los registros de consultas de la capacidad de iMessage se conservan hasta 25 días. Los registros de consultas de la capacidad de iMessage, siempre que estén disponibles, se pueden obtener con la correspondiente solicitud legalmente válida del país del solicitante.

U. App Apple TV

La app Apple TV permite a los clientes explorar, comprar, reproducir programas de TV y películas, y suscribirse a ellos desde Apple TV+, los canales de Apple TV, y las apps y los servicios de terceros. Es posible que el historial de compras y descargas esté disponible.

Las solicitudes de datos de clientes de la app Apple TV deben incluir el identificador del dispositivo Apple (número de serie, identidad internacional de equipo móvil [IMEI], identificador de equipo móvil [MEID] o identificador único global [GUID]) o la dirección de correo electrónico de la cuenta o el Apple ID pertinente. Si se desconoce la dirección de correo electrónico de la cuenta o el Apple ID, es necesario proporcionarle a Apple la información del cliente, como nombre completo y número de teléfono, o nombre completo y dirección física, para identificar la cuenta del cliente. Es posible que los oficiales de las agencias gubernamentales o los organismos de orden público también proporcionen un número de pedido de Apple válido o un número completo de tarjeta de crédito/débito asociado con compras de la app Apple TV. Es posible que también se proporcione el nombre de un cliente con estos parámetros, pero el nombre del cliente solo no es suficiente para obtener información.

Ten en cuenta lo siguiente: Cuando la solicitud legal incluye datos completos de la tarjeta de crédito/débito, por motivos relacionados con la seguridad de la información, dichos datos se deben enviar en un documento/archivo protegido con contraseña/encriptado (un archivo PDF y en formato

editable, por ejemplo, un documento de Numbers, Excel, Pages o Word) por correo electrónico a lawenforcement@apple.com y la contraseña se debe enviar en un correo electrónico separado. Asimismo, Apple no descargará solicitudes legales a través de ningún enlace enviado en un correo electrónico debido a los estándares de seguridad del sistema.

V. Iniciar sesión con Apple

Iniciar sesión con Apple es una forma más privada para que los clientes inicien sesión en apps y sitios web de terceros con el Apple ID existente del cliente. El botón Iniciar sesión con Apple en una app o un sitio web participante permite al cliente configurar una cuenta e iniciar sesión con el Apple ID. En lugar de usar una cuenta de redes sociales o completar formularios y seleccionar una contraseña nueva, el cliente puede tocar el botón Iniciar sesión con Apple, revisar su información e iniciar sesión de forma rápida y segura con Face ID, Touch ID o el código de su dispositivo. Puedes obtener más información en support.apple.com/es-lamr/HT210318.

Ocultar mi correo es una funcionalidad de Iniciar sesión con Apple. Usa el servicio de retransmisión de correo electrónico privado de Apple para crear y compartir una dirección de correo electrónico única y aleatoria que reenvía correos electrónicos a la dirección de correo electrónico personal de un cliente. Se puede obtener información básica del cliente con la correspondiente solicitud legalmente válida del país del solicitante.

IV. Preguntas frecuentes

P: ¿Puedo enviar un correo electrónico a Apple con preguntas sobre mi solicitud de información de un organismo de orden público?

R: Sí, las preguntas o las consultas sobre el proceso legal para entidades gubernamentales pueden enviarse por correo electrónico a lawenforcement@apple.com.

P: ¿Es necesario registrar un dispositivo en Apple para que funcione o para usarlo?

R: No, no es necesario que un dispositivo esté registrado en Apple para que funcione o para usarlo.

P: ¿Puede Apple proporcionarme el código de un dispositivo iOS que actualmente está bloqueado?

R: No, Apple no puede acceder al código de un cliente.

P: ¿Pueden ayudarme a devolver un dispositivo que se perdió o fue robado a la persona que lo perdió?

R: En estos casos, envía un correo electrónico a lawenforcement@apple.com. Incluye el número de serie del dispositivo (o el IMEI, si corresponde) en el correo electrónico y cualquier otra información pertinente. La información sobre cómo encontrar el número de serie está disponible aquí: support.apple.com/es-lamr/HT204308.

Si la información del cliente está disponible, Apple se comunicará con el cliente y le indicará cómo ponerse en contacto con los organismos de orden público para recuperar el dispositivo. Sin embargo, si no se puede determinar quién es el cliente a partir de la información disponible, es posible que se te pida que presentes una solicitud legalmente válida.

P: ¿Tiene Apple una lista de dispositivos perdidos o robados?

R: No, Apple no tiene una lista de dispositivos perdidos o robados.

P: ¿Qué se debe hacer con la información de la respuesta una vez que el organismo de orden público cerró la investigación/causa penal?

R: La información y los datos que se proporcionaron a las agencias gubernamentales o los organismos de orden público y que contienen información de identificación personal (incluidas las copias que se realizaron) se deben destruir después de que hayan finalizado completamente la investigación, la causa penal y todas las apelaciones relacionadas.

P: ¿Notifican a los clientes cuando reciben solicitudes de información de organismos de orden público relacionadas con ellos?

R: Sí, la política de aviso de Apple se aplica a las solicitudes de cuentas de organismos de orden público, agencias gubernamentales y entidades privadas. Apple notificará a los clientes y titulares de cuenta, a menos que ocurran las siguientes situaciones: cuando una orden de no divulgación o las leyes aplicables prohíban enviar un aviso; cuando Apple, a su entera discreción, crea razonablemente que dicho aviso puede representar un riesgo inminente de lesión grave o muerte para un miembro del público; cuando el caso se relacione con un asunto que ponga en peligro a un niño; o cuando el aviso no corresponda a los hechos subyacentes del caso.