



# Directrices sobre procedimientos legales

## Organismos gubernamentales y autoridades competentes fuera de Estados Unidos

Estas directrices se facilitan para su uso por parte de organismos gubernamentales y autoridades competentes fuera de Estados Unidos cuando necesiten información de entidades de Apple en la región o el país pertinentes acerca de dispositivos, productos y servicios de clientes de Apple. Apple actualizará estas directrices según sea necesario.

En estas directrices, Apple debe entenderse como la entidad pertinente responsable de la información de los clientes en una región o un país en concreto. Apple, como empresa multinacional, tiene ubicadas en varias jurisdicciones una serie de entidades jurídicas responsables de la información personal que recogen y que Apple Inc. trata en su nombre. Por ejemplo, la información de puntos de venta correspondiente a Apple Stores de fuera de Estados Unidos la controlan los establecimientos comerciales de Apple específicos de cada país. Es posible que estas entidades jurídicas ubicadas fuera de Estados Unidos también controlen la información personal relacionada con apple.com y los servicios multimedia de Apple, tal como se especifica en las condiciones de cada servicio ofrecido en una jurisdicción específica. Normalmente, las entidades jurídicas de Apple de fuera de Estados Unidos ubicadas en Australia, Canadá, Irlanda y Japón se responsabilizan de los datos de los clientes relacionados con los servicios de Apple en sus respectivas regiones.

Todas las demás peticiones de información relacionadas con clientes de Apple, incluidas las preguntas de los clientes acerca de la revelación de información, deben remitirse a la dirección [www.apple.com/es/privacy/contact/](http://www.apple.com/es/privacy/contact/). Estas directrices no se aplican a las peticiones que los organismos gubernamentales y las autoridades competentes de Estados Unidos hacen a Apple Inc.

Con respecto a las peticiones de información hechas por organismos gubernamentales y autoridades competentes, Apple cumple con la legislación que atañe a las entidades globales que controlan los datos y proporciona la información cuando la ley así lo exige. Todas las peticiones de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos sobre contenidos deben cumplir con la legislación correspondiente, incluida la Ley de Privacidad de las Comunicaciones Electrónicas (ley «ECPA», por sus siglas en inglés) de EE. UU., excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Una petición en virtud de un tratado bilateral de asistencia judicial o un acuerdo ejecutivo, o de la Ley de Aclaración del Uso Legítimo de los Datos en el Extranjero (ley «CLOUD», por sus siglas en inglés) de EE. UU., se ajusta a la ECPA. Apple solo proporcionará los contenidos del cliente tal y como aparecen en su cuenta en respuesta a un procedimiento legalmente válido de este tipo.

Con respecto a las peticiones de entidades privadas, Apple cumple con la legislación que atañe a las entidades locales que controlan los datos de los clientes y proporciona la información cuando la ley así lo exige.

Apple tiene un proceso centralizado para recibir, seguir, tratar y responder peticiones legales legítimas de organismos gubernamentales, autoridades competentes y entidades privadas desde que se reciben hasta la facilitación de una respuesta. Un equipo formado de nuestro departamento jurídico revisa y evalúa todas las peticiones que se reciben, y se opone, recusa o rechaza las peticiones que Apple considera faltas de fundamento jurídico válido o que no resultan claras, son inadecuadas o demasiado generales.

Apple proporciona respuestas a las autoridades competentes solicitantes en la dirección de correo electrónico oficial del agente que realiza la solicitud. La conservación de las pruebas de acuerdo con las respuestas proporcionadas por Apple es responsabilidad de la agencia de cumplimiento de la ley solicitante.

# **ÍNDICE**

## **I. Información general**

## **II. Peticiones legales hechas a Apple**

- A. Peticiones de información hechas por organismos gubernamentales y autoridades competentes
- B. Gestión y respuesta a peticiones de información hechas por organismos gubernamentales y autoridades competentes
- C. Peticiones de conservación
- D. Peticiones de urgencia
- E. Peticiones de restricción o eliminación de cuenta
- F. Aviso al cliente

## **III. Información en posesión de Apple**

- A. Registro de dispositivos
- B. Registros del servicio de atención al cliente
- C. Servicios multimedia de Apple
- D. Transacciones en un Apple Store
- E. Pedidos de apple.com
- F. Tarjetas regalo
- G. Apple Pay
- H. iCloud
- I. Buscar
- J. AirTag y programa de accesorios de la red Buscar
- K. Extracción de datos de dispositivos iOS bloqueados con código
- L. Solicitud de dirección IP
- M. Otra información disponible sobre dispositivos
- N. Peticiones de los datos de videovigilancia de un Apple Store
- O. Game Center
- P. Activación de dispositivos iOS
- Q. Registros de conexión
- R. Registros de Mi ID de Apple 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 de comunicación móvil y multimedia, ordenadores personales y reproductores de música digital portátiles; también vende una gama de software relacionado, servicios, periféricos, soluciones de redes y contenido digital y aplicaciones de terceros. La oferta de productos y servicios de Apple incluye Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, una selección de aplicaciones de software para particulares y profesionales, los sistemas operativos iOS y macOS X, iCloud y diferentes accesorios, servicios y opciones de soporte. Apple también vende y distribuye contenido digital y aplicaciones a través de Apple Music, App Store, Apple Books y Mac App Store. Apple guarda la información de los clientes de conformidad con la [política de privacidad](#) de Apple y las [condiciones de servicio](#) aplicables a un servicio determinado. Apple se compromete a mantener la privacidad de los clientes de productos y servicios de Apple (en adelante, «clientes de Apple»). En este sentido, salvo en las situaciones de carácter urgente establecidas en la ley, no se revelará información sobre clientes de Apple sin un procedimiento legal válido.

La información incluida en estas directrices pretende informar a los organismos gubernamentales y las autoridades competentes de fuera de Estados Unidos acerca de los procedimientos legales que Apple requiere para revelar información electrónica. Estas directrices no pretenden proporcionar asesoría legal. En el apartado Preguntas frecuentes de estas directrices está dirigida a proporcionar respuestas a algunas de las preguntas más comunes que Apple recibe. Ni las presentes directrices ni el apartado Preguntas frecuentes cubren todas las circunstancias que pueden darse.

Si tiene más preguntas, póngase en contacto con [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

La dirección de correo anterior está destinada para uso exclusivo del personal de organismos gubernamentales y autoridades competentes. Quien decida enviar un mensaje a esta dirección, debe hacerlo desde una dirección de correo electrónico válida y oficial perteneciente a un organismo gubernamental o una autoridad competente.

Las peticiones legales hechas a Apple deben solicitar información sobre un dispositivo Apple o cliente determinado y los servicios específicos que Apple puede proporcionar a dicho cliente. Apple puede proporcionar información sobre el dispositivo Apple o el cliente si la información solicitada está aún en posesión de Apple de conformidad con las políticas de retención de datos. Apple conserva los datos de acuerdo con las pautas especificadas en los subapartados de «Información en posesión de Apple» de este documento. Todos los demás datos se conservan durante el tiempo necesario para cumplir los fines establecidos en nuestra [política de privacidad](#). Los organismos gubernamentales y las autoridades competentes deben ser lo más concretos y específicos posible a la hora de formular sus peticiones para evitar interpretaciones erróneas o que dichas peticiones se objetan, recusen o rechacen por no estar claras, no ser apropiadas o ser demasiado amplias. Todas las peticiones de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos sobre contenidos deben cumplir con la legislación correspondiente, incluida la ley ECPA estadounidense, excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Una petición en virtud de un tratado bilateral de asistencia judicial o un acuerdo ejecutivo, o de la ley CLOUD estadounidense, se ajusta a la ECPA. Apple solo proporcionará los contenidos del cliente tal y como aparecen en su cuenta en respuesta a un procedimiento legalmente válido de este tipo.

Nada de lo establecido en estas directrices pretende crear derechos susceptibles de aplicación contra Apple. Además, las políticas de Apple están sujetas a actualizaciones o cambios futuros sin previo aviso a los organismos gubernamentales ni a las autoridades competentes.

## II. Peticiones legales hechas a Apple

### A. Peticiones de información hechas por organismos gubernamentales y autoridades competentes

Apple acepta las peticiones de información legalmente válidas que los organismos gubernamentales y las autoridades competentes envíen por correo electrónico, siempre que se envíen desde la dirección oficial del organismo gubernamental o la autoridad competente que realiza la petición. El personal de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos que transmita una petición de información a Apple debe completar una [plantilla de petición de información de organismos gubernamentales y autoridades competentes](#) y enviarla directamente desde su dirección de correo electrónico válida y oficial perteneciente a un organismo gubernamental o una autoridad competente a la dirección de correo: [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

La dirección de correo anterior está destinada para uso exclusivo del personal de organismos gubernamentales y autoridades competentes. Si la petición contiene cinco identificadores o más, como números de serie/IMEI de dispositivos, varios ID de Apple, direcciones de correo electrónico o números de factura/pedido, dichos identificadores deben estar en formato editable (por ejemplo, en un documento Numbers, Excel, Pages o Word). Estos identificadores suelen ser necesarios para buscar información relacionada con dispositivos, cuentas o transacciones financieras.

**Nota:** De acuerdo con las normas de seguridad del sistema, Apple no descargará peticiones legales ni documentos relacionados desde ningún enlace enviado en un correo electrónico.

Para que Apple pueda revelar información sobre clientes en respuesta a una petición de una autoridad competente, es necesario que el agente que realiza la petición indique el fundamento jurídico que autoriza a la autoridad competente a obtener información relevante en forma de datos personales de un responsable del tratamiento de datos, como Apple. He aquí algunos ejemplos de peticiones que Apple considera legalmente válidas: Production Orders (Australia, Canadá y 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) y Personal Data Request, Orders, Warrants y Communications Data Authorisations (Reino Unido), así como órdenes o peticiones de tribunales de otros países.

### B. Gestión y respuesta a peticiones de información hechas por organismos gubernamentales y autoridades competentes

Apple revisa detenidamente todas las peticiones legales para asegurarse de que exista un fundamento jurídico válido para cada petición y cumple con las peticiones legalmente válidas. Cuando Apple determine que no hay un fundamento jurídico válido, o cuando una petición no resulte clara, sea inadecuada o demasiado general, Apple se opondrá, recusará o rechazará la petición.

Para fines de tratamiento y debido a limitaciones del sistema, Apple no puede aceptar peticiones legales que contengan más de 25 identificadores de cuentas. Si una autoridad competente presenta peticiones legales con más de 25 identificadores de cuentas, Apple responderá a los primeros 25 y la autoridad competente deberá volver a presentar una nueva petición legal para los otros identificadores.

### C. Peticiones de conservación

Todas las peticiones de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos sobre contenidos deben cumplir con la legislación correspondiente, incluida la ley ECPA estadounidense, excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Una petición en virtud de un tratado bilateral de asistencia judicial o un acuerdo ejecutivo o de la ley CLOUD estadounidense se ajusta a la ECPA. Las peticiones de conservación de datos con carácter inmediato antes del inicio de un proceso conforme a la ECPA deben enviarse por correo electrónico a [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

Las peticiones de conservación deberán incluir el ID de Apple o la dirección de correo electrónico de la cuenta pertinente, el nombre completo y el número de teléfono y/o el nombre completo y la dirección física del cliente de la cuenta de Apple en cuestión. Cuando haya recibido una petición de conservación, Apple conservará durante 90 días un único registro de los datos del cliente existentes y disponibles en el momento de la petición. Tras este periodo de 90 días, los datos conservados se eliminarán automáticamente del servidor de almacenamiento. No obstante, este periodo puede ampliarse otros 90 días en caso de recibir una nueva petición. Cuando se intenten entregar más de dos peticiones de conservación para la misma cuenta, la segunda petición se tratará como una petición de ampliación de la conservación original, no como una conservación independiente de nuevos datos.

## **D. Peticiones de urgencia**

Apple considera que una petición es de urgencia cuando guarda relación con circunstancias que implican amenazas graves e inminentes para la vida/seguridad de personas, la seguridad de un estado o la seguridad de infraestructuras/instalaciones críticas.

Si el agente del organismo gubernamental o la autoridad competente que realiza la petición proporciona datos suficientes para confirmar que dicha petición está motivada por circunstancias urgentes que cumplen alguno de los criterios especificados anteriormente, Apple examinará la petición con carácter urgente.

Para pedir a Apple que revele voluntariamente información de manera urgente, el agente del organismo gubernamental o la autoridad competente que realiza la petición debe rellenar la plantilla [«Emergency Government & Law Enforcement Information Request»](#) y enviarla directamente desde su dirección de correo electrónico oficial del organismo gubernamental o la autoridad competente a [exigent@apple.com](mailto:exigent@apple.com), con las palabras «Emergency Request» (Petición de urgencia) en el asunto.

Si un organismo gubernamental o una autoridad competente piden datos de clientes en respuesta a una petición de urgencia de información de organismos gubernamentales y autoridades competentes, Apple podrá ponerse en contacto con un supervisor del organismo gubernamental o de la autoridad competente que presentó la petición para que confirme el carácter legítimo de la petición. El organismo gubernamental o la autoridad competente que realicen la petición de urgencia de información de organismos gubernamentales y autoridades competentes deberán facilitar la información de contacto del supervisor en la petición.

Si un organismo gubernamental o una autoridad competente necesitan contactar con Apple para una petición de urgencia, deberán ponerse en contacto con el Centro Global de Operaciones de Seguridad (GSOC) de Apple en el 001 408 974-2095. Este número de teléfono ofrece asistencia en varios idiomas.

## **E. Peticiones de restricción o eliminación de cuenta**

Si un organismo gubernamental o una autoridad competente solicitan a Apple que restrinja o elimine el ID de Apple de un cliente, deben hacerlo por medio de una orden judicial u otro procedimiento legal equivalente del país correspondiente (a menudo, una sentencia condenatoria o resolución judicial) que demuestre que la cuenta que debe restringirse o eliminarse se ha utilizado ilegítimamente.

Apple examina detenidamente todas las peticiones procedentes de organismos gubernamentales y autoridades competentes para comprobar que se fundamentan en una base jurídica válida. 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 va a restringir o eliminar se ha utilizado de forma ilegal, Apple rechazará o impugnará la solicitud.

Cuando Apple reciba una orden judicial u otro procedimiento legal equivalente del país correspondiente (a menudo, una sentencia condenatoria o resolución judicial) de un organismo gubernamental o una autoridad competente que demuestre que la cuenta que debe restringirse o eliminarse se ha utilizado ilegítimamente, Apple tomará las medidas solicitadas para restringir o eliminar la cuenta de conformidad con la orden judicial y aconsejará al organismo u autoridad pertinente de manera acorde.

## **F. Aviso al cliente**

Apple notificará a sus clientes que ha recibido una petición de información con validez legal referente a su cuenta de Apple realizada por un organismo gubernamental o una autoridad competente, salvo cuando dicha notificación se prohíba explícitamente en la petición legal válida, en la orden judicial recibida o según la legislación aplicable; cuando Apple considere, a su entera discreción, que la notificación puede poner en riesgo de lesión o muerte a una persona en concreto; cuando el caso esté relacionado con situaciones de peligro para un menor, o cuando la notificación no sea aplicable a las circunstancias del caso.

Transcurridos 90 días, Apple notificará a posteriori la existencia de revelaciones de urgencia, salvo si dicha notificación se prohíbe explícitamente por orden judicial o según la legislación aplicable; cuando Apple considere, a su entera discreción, que la notificación puede poner en riesgo de lesión o muerte a una persona o grupo de personas en concreto, o cuando el caso esté relacionado con situaciones de peligro para un menor. Apple notificará a posteriori cuando venza el periodo de no revelación especificado en una orden judicial a menos que, a su entera discreción, considere que la notificación puede poner en riesgo de lesión o muerte a una persona o grupo de personas en concreto; cuando el caso esté relacionado con situaciones de peligro para un menor, o cuando la notificación no sea aplicable a las circunstancias del caso.

Apple notificará a sus clientes si ha restringido o eliminado su cuenta de Apple en respuesta a una orden judicial (a menudo, una sentencia condenatoria o resolución judicial) que demuestre que dicha cuenta se ha utilizado ilegítimamente o de una forma que incumple las condiciones de servicio de Apple, salvo cuando dicha notificación se prohíba explícitamente en el propio procedimiento legal, en la orden judicial recibida o según la legislación aplicable; cuando el caso esté relacionado con situaciones de peligro para un menor; cuando Apple considere, a su entera discreción, que la notificación puede poner en riesgo de lesión o muerte a una persona o grupo de personas en concreto, o cuando la notificación no sea aplicable a las circunstancias del caso.

### **III. Información en posesión de Apple**

En este apartado se abordan los tipos generales de información que pueden obtenerse de Apple en el momento de publicación de estas directrices.

#### **A. Registro de dispositivos**

El registro básico o la información del cliente, como el nombre, la dirección postal, la dirección de correo electrónico y el número de teléfono, se proporcionan a Apple al registrar un dispositivo Apple anterior a las versiones iOS 8 y macOS Sierra 10.12. Apple no verifica esta información y es posible que sea inexacta o que no se corresponda con el propietario del dispositivo. La información de registro de los dispositivos que funcionan con iOS 8 y versiones posteriores, así como la de los Mac que funcionan con macOS Sierra 10.12 y versiones posteriores, se recibe cuando un cliente asocia un dispositivo a un ID de Apple en iCloud. Es posible que esta información sea inexacta o que no se corresponda con el propietario del dispositivo. La información de registro, si está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

Tenga en cuenta que los números de serie del dispositivo Apple no contienen las letras «O» ni «I»; en cambio, Apple utiliza los números 0 (cero) y 1 (uno) en los números de serie. Las peticiones de números de serie con la letra «O» o «I» no generarán ningún resultado. En los casos en los que una petición legal incluya cinco números de serie o más, Apple solicita que dichos números de serie se envíen también en formato electrónico editable (por ejemplo, en un documento Numbers, Excel, Pages o Word).

#### **B. Registros del servicio de atención al cliente**

Apple puede proporcionar los contactos que los clientes hayan tenido con el servicio de atención al cliente de Apple con respecto a un dispositivo o servicio. Esta información puede incluir registros de interacciones del soporte técnico con los clientes con respecto a un dispositivo o servicio de Apple específico. Además, también puede estar disponible la información relativa al dispositivo, la garantía y la reparación. Si esta información está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

#### **C. Servicios multimedia de Apple**

App Store, Apple Music, la app Apple TV, Apple Podcasts y Apple Books (los «servicios multimedia de Apple») son aplicaciones de software que los clientes usan para organizar y reproducir apps y contenido digital de música y vídeo, así como para transmitir contenido. Los servicios multimedia de Apple también ofrecen contenido que los clientes pueden descargar a sus ordenadores y dispositivos iOS. Cuando un cliente abre una cuenta de Apple, puede proporcionar a Apple información básica sobre él, como su nombre, dirección física, dirección de correo electrónico y número de teléfono. También podrá estar disponible información sobre conexiones para realizar transacciones de compra o descarga en servicios multimedia de Apple y conexiones para obtener actualizaciones o nuevas descargas. La información sobre la dirección IP puede restringirse a los 18 últimos meses. Si se dispone de la información de clientes de servicios multimedia de Apple y los registros de conexión con direcciones IP, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.



Las peticiones de datos de servicios multimedia de Apple deben incluir el identificador del dispositivo Apple (número de serie, IMEI, MEID o GUID) o el ID de Apple o la dirección de correo electrónico de la cuenta correspondiente. En caso de no disponer del ID de Apple o la dirección de correo electrónico de la cuenta, será necesario proporcionar a Apple información del cliente de servicios multimedia de Apple, ya sean su nombre completo y su número de teléfono o su nombre completo y su dirección física, para poder identificar la cuenta de servicios multimedia de Apple asociada. Los agentes del organismo gubernamental o la autoridad competente también podrán proporcionar un número de pedido de servicios multimedia de Apple válido o el número completo de la tarjeta de débito o crédito asociada a la adquisición de servicios multimedia de Apple. También podrá facilitarse el nombre de un cliente en combinación con estos parámetros, pero el nombre del cliente por sí solo no es suficiente para obtener información.

**Nota:** Por motivos de seguridad de los datos, cuando su petición legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, se debe enviar la contraseña en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## D. Transacciones en un Apple Store

Las transacciones en el punto de venta son transacciones en efectivo, con tarjeta de crédito o débito o con tarjeta regalo que se realizan en un Apple Store. Las peticiones de acceso a los registros de un punto de venta deben incluir el número completo de la tarjeta de crédito o débito utilizada y pueden incluir también otra información relevante, como la fecha y la hora de la transacción, el importe y los artículos adquiridos. La información sobre el tipo de tarjeta asociada a una compra determinada, el nombre del comprador, la dirección de correo electrónico, la fecha y la hora de la transacción, el importe de la transacción y la ubicación de la tienda, si está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

Las peticiones de copias de recibos deben incluir el número de transacción de la tienda asociado a la compra o las compras correspondientes y, en caso de que dichas copias estén disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

**Nota:** Por motivos de seguridad de los datos, cuando su petición legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, se debe enviar la contraseña en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## E. Pedidos de apple.com

Apple conserva información sobre pedidos realizados en apple.com, que puede incluir el nombre del comprador, la dirección de envío, el número de teléfono, la dirección de correo electrónico, los productos adquiridos, la cantidad adquirida y la dirección IP desde la que se realizó la compra. Las peticiones de información pertenecientes a pedidos de apple.com deben incluir un número completo de tarjeta de crédito o débito o un número de pedido, o bien el número de serie del artículo adquirido. También podrá facilitarse el nombre de un cliente en combinación con estos parámetros, no obstante, el nombre del cliente por sí solo no es suficiente para obtener información. Las peticiones de

información sobre pedidos realizados en apple.com también pueden incluir el ID de Apple o la dirección de correo electrónico de la cuenta correspondiente. En caso de no disponer del ID de Apple ni de la dirección de correo electrónico de la cuenta, Apple requiere algunos datos del cliente, ya sean su nombre completo y el número de teléfono, o su nombre completo y la dirección física para poder identificar la cuenta de Apple asociada. La información de compra de los pedidos realizados en apple.com, en caso de estar disponible, se puede obtener mediante una petición legalmente válida para el país del solicitante.

**Nota:** Por motivos de seguridad de los datos, cuando su petición legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, se debe enviar la contraseña en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## F. Tarjetas regalo

Las tarjetas regalo del Apple Store y las del App Store y iTunes tienen un número de serie. Estos números de serie tienen diferentes formatos, según factores como el diseño o la fecha y hora de emisión. Apple puede ofrecer información disponible acerca de tarjetas regalo del Apple Store y las del App Store y iTunes en respuesta a la petición legalmente válida adecuada para el país del solicitante. En los casos en que una petición legal incluya cinco números de serie de tarjetas regalo o más, Apple solicita que estos datos se envíen en un documento protegido por contraseña o cifrado (por ejemplo, Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, la contraseña se debe enviar en un correo electrónico por separado.

### i. Tarjetas regalo del Apple Store

Las tarjetas regalo del Apple Store pueden usarse para comprar artículos en apple.com o en un Apple Store. Los registros disponibles pueden incluir información sobre el comprador de la tarjeta regalo (si la ha adquirido de Apple y no de un tercero), las transacciones de compra asociadas y los artículos adquiridos. En ocasiones, es posible que Apple pueda cancelar o suspender una tarjeta regalo del Apple Store dependiendo del estado de la tarjeta en cuestión. Si la información sobre una tarjeta regalo del Apple Store está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

**Nota:** Por motivos de seguridad de los datos, si su petición legal contiene datos completos de una tarjeta regalo del Apple Store, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, la contraseña deberá enviarse en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## ii. Tarjetas regalo del App Store y iTunes

Las tarjetas regalo del App Store y iTunes pueden usarse en Apple Music, el App Store, Apple Books y el Mac App Store. Con el número de serie, Apple puede determinar si una tarjeta regalo del App Store y iTunes se ha activado (adquirido en el punto de venta de un establecimiento comercial) o canjeado (añadido al saldo a favor en la tienda de una cuenta de Apple).

Cuando se activa una tarjeta regalo del App Store y iTunes, los registros disponibles podrán incluir el nombre de la tienda, el lugar, la fecha y la hora. Cuando se canjea una tarjeta regalo del App Store y iTunes, los registros disponibles podrán incluir información del cliente sobre la cuenta de Apple relacionada, la fecha y hora de activación o canje, y la dirección IP desde la que se ha realizado el canje. En ocasiones, es posible que Apple pueda deshabilitar una tarjeta regalo del App Store y iTunes Store dependiendo del estado de la tarjeta en cuestión. Si la información sobre una tarjeta regalo del App Store y iTunes está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

**Nota:** Por motivos de seguridad de los datos, si su petición legal contiene datos completos de una tarjeta regalo del App Store y iTunes, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, la contraseña deberá enviarse en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## G. Apple Pay

Las transacciones de Apple Pay realizadas en establecimientos comerciales (por ejemplo, en el caso de comunicaciones NFC o contactless) o en apps o puntos de venta en línea se autentican de manera segura en el dispositivo del cliente y se envían cifradas al vendedor o procesador de pagos del vendedor. Aunque la seguridad de las transacciones se verifica en un servidor de Apple, Apple no procesa pagos o transacciones en tienda de este tipo, ni tampoco los números completos de tarjetas de débito o crédito asociadas a compras realizadas con Apple Pay. Esta información podrá obtenerse del banco emisor pertinente, la red de pagos o el vendedor.

Encontrará más información acerca de los países y regiones que admiten Apple Pay en [support.apple.com/es-es/HT207957](https://support.apple.com/es-es/HT207957).

Para solicitar datos de transacciones para compras realizadas en un Apple Store o a través de apple.com, Apple necesita el número de la cuenta principal del dispositivo (DPAN) que se utilizó para la transacción. El DPAN tiene 16 dígitos y se puede obtener en el banco emisor. Nota: El DPAN se utiliza en las transacciones de pago sin contacto con el comerciante en el lugar del propio número de la tarjeta de crédito o débito (FPAN/PAN de fondos). El procesador de pagos convierte el DPAN en el FPAN correspondiente. Con la información del DPAN correspondiente, Apple podrá llevar a cabo a una búsqueda razonable para encontrar información mediante su sistema de punto de venta. Estos registros, en el caso de que estén disponibles, se pueden obtener mediante la correspondiente solicitud legalmente válida para el país del solicitante.

Apple podrá facilitar información de Apple Pay acerca de los tipos de tarjetas de crédito o débito que un cliente haya añadido a Apple Pay, junto con información del cliente. Si esta información está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Para pedir esta información, Apple necesita un identificador del dispositivo (número de serie de Apple, SEID, IMEI o MEID) o un ID de Apple o dirección de correo electrónico de la cuenta.

**Nota:** Por motivos de seguridad de los datos, si su solicitud legal contiene el DPAN, los datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, la contraseña deberá enviarse en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## H. iCloud

iCloud es el servicio en la nube de Apple que permite a los clientes acceder a sus fotos, documentos y muchos otros contenidos desde todos sus dispositivos. También permite a los clientes hacer copias de seguridad de sus dispositivos iOS y iPadOS en iCloud. Con este servicio, los clientes pueden configurar una cuenta de correo 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 se cifran en la ubicación del servidor. Para los datos que Apple puede descifrar, Apple conserva las claves de cifrado en sus centros de datos de EE. UU. Apple no recibe ni conserva claves de cifrado para los datos cifrados de punto a punto del cliente.

iCloud es un servicio basado en clientes. Las peticiones de datos de iCloud deben incluir el ID de Apple o la dirección de correo electrónico de la cuenta correspondiente. En caso de no disponer del ID de Apple o la dirección de correo electrónico de la cuenta, Apple requiere algunos datos del cliente, ya sean su nombre completo y el número de teléfono, o su nombre completo y la dirección física para poder identificar la cuenta de Apple asociada. Cuando solo se facilite un número de teléfono o ID de Apple o la dirección de correo electrónico, se podrá producir información disponible sobre las cuentas verificadas relacionadas con estos criterios.

I. Es posible obtener la información siguiente de iCloud:

### I. Información del cliente

Cuando un cliente configura una cuenta de iCloud, puede proporcionar a Apple información básica sobre él, como su nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, también puede estar disponible información sobre conexiones de prestaciones de iCloud.

Si la información del cliente y los registros de conexión del cliente de iCloud están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Los registros de conexión se conservan como máximo durante 25 días.

### I. Registros de correo

Los registros de correo incluyen información sobre las comunicaciones entrantes y salientes, incluidas la hora, la fecha, las direcciones de correo del remitente y las direcciones de correo

del destinatario. Los registros de correo de iCloud se conservan como máximo durante 25 días y, si están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **II. Contenidos de correo electrónico y otros contenidos de iCloud, Mis Fotos en streaming, Fototeca de iCloud, iCloud Drive, contactos, calendarios, favoritos, historial de navegación de Safari, historial de búsqueda de Mapas, mensajes y copias de seguridad de dispositivos iOS**

En iCloud se almacenan contenidos que el cliente ha decidido mantener en la cuenta mientras está activa. Apple no retiene contenido eliminado después de haberlo borrado de sus servidores. Los contenidos de iCloud pueden incluir correos electrónicos, fotos almacenadas, documentos, contactos, calendarios, favoritos, el historial de navegación de Safari, el historial de búsqueda de Mapas, los mensajes y las copias de seguridad de dispositivos iOS. Las copias de seguridad de dispositivos iOS pueden contener fotos y vídeos del Carrete, ajustes del dispositivo, datos de apps, iMessage, Business Chat, mensajes SMS y MMS y mensajes en el buzón de voz. Todos los datos de contenido de iCloud almacenados por Apple se cifran en la ubicación del servidor. Para los datos que Apple puede descifrar, Apple conserva las claves de cifrado en sus centros de datos de EE. UU. Apple no recibe ni conserva claves de cifrado para los datos cifrados de punto a punto del cliente.

Todas las peticiones de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos sobre contenidos deben cumplir con la legislación correspondiente, incluida la ley ECPA estadounidense, excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Una petición en virtud de un tratado bilateral de asistencia judicial o un acuerdo ejecutivo, o de la ley CLOUD estadounidense, se ajusta a la ECPA. Apple solo proporcionará los contenidos del cliente tal y como aparecen en su cuenta en respuesta a una solicitud legalmente válida de este tipo.

## **II. Protección de Datos Avanzada**

La Protección de Datos Avanzada para iCloud es una prestación que utiliza cifrado de punto a punto para proteger los datos de iCloud con el nivel más alto de seguridad de datos de Apple. Para los usuarios que habilitan la Protección de Datos Avanzada para iCloud, puede que los datos de iCloud disponibles sean limitados. Encontrará más información sobre la Protección de Datos Avanzada en [support.apple.com/es-es/guide/security/sec973254c5f/web](https://support.apple.com/es-es/guide/security/sec973254c5f/web) y [support.apple.com/es-es/HT212520](https://support.apple.com/es-es/HT212520). La siguiente información puede estar disponible en iCloud si un usuario ha habilitado la Protección de Datos Avanzada para iCloud:

### **a. Información del cliente**

Cuando un cliente configura una cuenta de iCloud, puede proporcionar a Apple información básica sobre él, como su nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, también puede estar disponible información sobre conexiones de prestaciones de iCloud. Si la información del cliente y los registros de conexión del cliente de iCloud están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Los registros de conexión se conservan como máximo durante 25 días.

### **b. Registros de correo**

Los registros de correo incluyen información sobre las comunicaciones entrantes y salientes, incluidas la hora, la fecha, las direcciones de correo del remitente y las direcciones de correo del destinatario. Los registros de correo de iCloud se conservan

como máximo durante 25 días y, si están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

### **c. Contenidos de correo electrónico y otros contenidos de iCloud**

Para los usuarios que han habilitado la Protección de Datos Avanzada, iCloud almacena el contenido del correo electrónico, los contactos y los calendarios que el cliente ha decidido mantener en la cuenta mientras está activa. Estos datos se pueden proporcionar, tal como están en la cuenta del cliente, con la solicitud legalmente válida adecuada para el país del solicitante. Apple almacena estos datos limitados y, además, los cifra en la ubicación del servidor. Para los datos que Apple puede descifrar, Apple conserva las claves de cifrado en sus centros de datos de EE. UU. Apple no recibe ni conserva claves de cifrado para los datos cifrados de punto a punto del cliente.

La Protección de Datos Avanzada utiliza cifrado de punto a punto y Apple no puede descifrar cierto contenido de iCloud, como Fotos, iCloud Drive, Copia de seguridad, Notas y Favoritos de Safari. En algunas circunstancias, Apple puede retener información limitada relacionada con estos servicios de iCloud que se puede obtener, si está disponible, con la solicitud legalmente válida correspondiente para el país del solicitante.

## **III. Relay Privado de iCloud**

Relay Privado de iCloud es un servicio de privacidad en internet que se ofrece como parte de una suscripción a iCloud+. Relay Privado protege la navegación web de los usuarios en Safari, las consultas de resolución de DNS (espacio de nombres de dominio) y el tráfico de apps http sin cifrar. 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 utilizar Relay Privado de iCloud. Encontrará más información sobre Relay Privado en [support.apple.com/es-es/HT212614](https://support.apple.com/es-es/HT212614) y [www.apple.com/privacy/docs/iCloud\\_Private\\_Relay\\_Overview\\_Dec2021.PDF](https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF).

Cuando Relay Privado está habilitado, las solicitudes de navegación web del usuario se envían a través de dos relays de internet seguros e independientes. La dirección IP del usuario está visible para el proveedor de red del usuario y el primer relay, operado por Apple. Los registros DNS del usuario están cifrados, por lo que ninguna de las partes puede ver la dirección del sitio web que el usuario está intentando visitar. El segundo relay, operado por un proveedor de contenido externo, genera una dirección IP temporal, descifra el nombre del usuario del sitio web solicitado y conecta al usuario con el sitio. Relay Privado valida que el cliente que se conecta es un iPhone, iPad o Mac. Relay Privado sustituye la dirección IP original del usuario por una asignada del rango de direcciones IP utilizadas por el servicio. La dirección IP de relay asignada puede compartirse entre más de un usuario de Relay Privado en la misma área.

Cuando las solicitudes de navegación web del usuario utilizan Relay Privado, Apple no puede determinar la dirección IP del cliente o la cuenta de usuario correspondiente a partir de las direcciones IP de Relay Privado. Apple no tiene información que proporcionar sobre el ID de Apple asociado con la dirección IP de Relay Privado.

Nota: Relay Privado de iCloud no está disponible en todos los países o regiones. Si los usuarios tienen Relay Privado habilitado y viajan a algún lugar en el que no está disponible, se desactivará automáticamente y se volverá a activar cuando los usuarios vuelvan a entrar en un país o región que lo admita.

## **I. Buscar**



Buscar es una prestación que pueden activar los usuarios y que permite a los clientes de iCloud localizar su iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac o AirTag en caso de pérdida o robo. También les permite tomar determinadas medidas, como activar el modo Perdido del dispositivo, bloquearlo o borrar todos sus contenidos. Encontrará más información sobre este servicio en [www.apple.com/es/icloud/find-my/](http://www.apple.com/es/icloud/find-my/).

Para que un usuario que ha perdido su dispositivo pueda usar Buscar, debe haber habilitado esta prestación en el dispositivo en concreto antes de perderlo. La prestación Buscar no puede activarse en un dispositivo después de perderlo, de forma remota ni si lo solicita un organismo gubernamental o una autoridad competente. La información de los servicios de ubicación de un dispositivo se almacena en el propio dispositivo, por lo que Apple no puede obtenerla de ningún dispositivo en concreto. La información de los servicios de localización de un dispositivo localizado con la prestación Buscar se proporciona únicamente al cliente y Apple no dispone de los contenidos de los mapas ni de alertas transmitidas a través del servicio. En el enlace de soporte siguiente se ofrece información y los pasos que pueden seguir los clientes si han perdido o les han robado su dispositivo iOS: [support.apple.com/es-es/HT201472](http://support.apple.com/es-es/HT201472).

Los registros de conexión de Buscar están disponibles durante un periodo máximo de 25 días y, si están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Si la información sobre las peticiones recibidas a través de Buscar para bloquear un dispositivo o borrar sus contenidos de forma remota está disponible, podrá obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **J. AirTag y programa de accesorios de la red Buscar**

Con la app Buscar del iPhone, iPad, iPod touch y Mac, los clientes pueden encontrar fácilmente objetos personales. Basta con ponerles un AirTag o usar un producto que forme parte del programa de accesorios de la red Buscar. Con AirTag y iOS 14.5 o macOS 11.3, o versiones posteriores, los clientes reciben ayuda para buscar objetos personales perdidos (llaves, mochilas, maletas, etc.) mediante la app Buscar. El AirTag debe estar en el rango de alcance de Bluetooth del iPhone, iPad o iPod touch con el que esté emparejado para emitir un sonido, o utilizar la Búsqueda de Precisión con iPhone compatibles. Si no está cerca del propietario, se puede consultar la posición aproximada del AirTag, siempre que esté al alcance de un dispositivo de la red Buscar, que integran cientos de millones de dispositivos Apple en todo el mundo. Encontrará más información en: [support.apple.com/es-es/HT212227](http://support.apple.com/es-es/HT212227) y [support.apple.com/es-es/HT210967](http://support.apple.com/es-es/HT210967).

El programa de accesorios de la red Buscar pone a disposición esta red para productos de otros fabricantes (bicicletas, auriculares, etc.) para que utilicen el servicio y que sus clientes puedan localizar los productos compatibles con la app Buscar con iOS 14.3 y macOS 11.1, o versiones posteriores.

Para añadir un AirTag o productos compatibles de otros fabricantes en la pestaña «Objetos» de la app Buscar, los clientes necesitan un ID de Apple, estar registrados en una cuenta de iCloud que tenga Buscar activado y registrar el AirTag o el producto compatible en su ID de Apple. La interacción está cifrada de punto a punto y Apple no puede ver la posición de ningún AirTag ni de ningún producto de otro fabricante. Encontrará más información en [support.apple.com/es-es/HT211331](http://support.apple.com/es-es/HT211331).

Con un número de serie, Apple puede proporcionar los datos de la cuenta enlazada para responder a una petición legalmente válida adecuada para el país del solicitante. El historial de enlace de los AirTag

está disponible hasta 25 días. En este enlace se explica dónde encontrar el número de serie de un AirTag: [support.apple.com/es-es/HT211658](https://support.apple.com/es-es/HT211658).

Tenga en cuenta que los números de serie del dispositivo Apple no contienen las letras «O» ni «I»; en cambio, Apple utiliza los números 0 (cero) y 1 (uno) en los números de serie. Las peticiones de números de serie con la letra «O» o «I» no generarán ningún resultado. En los casos en los que una petición legal incluya cinco números de serie o más, Apple solicita que dichos números de serie se envíen también en formato electrónico editable (por ejemplo, en un documento Numbers, Excel, Pages o Word).

## **K. Extracción de datos de dispositivos iOS bloqueados con código**

Apple no puede obtener los datos de los dispositivos que tienen iOS 8.0 o una versión posterior, ya que los datos normalmente solicitados por las autoridades competentes están cifrados y Apple no dispone de la clave de cifrado. El iPhone 6 y todos los modelos posteriores ejecutan iOS 8.0 o una versión posterior.

En el caso de los dispositivos que ejecutan las versiones 4 a 7 de iOS y en función del estado del dispositivo en cuestión, Apple puede extraer datos de iOS en virtud de la legislación de California en materia de privacidad de las comunicaciones electrónicas (CalECPA, secciones 1546-1546.4 del código penal de California). Para que Apple pueda extraer datos de iOS de un dispositivo que cumpla con estos criterios, la autoridad competente deberá obtener una orden de registro por causa probable de conformidad con la CalECPA. Aparte de lo establecido en la CalECPA, Apple no ha identificado ninguna autoridad legal que le pueda exigir la extracción de datos en calidad de tercero durante el curso de una investigación de la autoridad competente.

## **L. Solicitud de dirección IP**

Antes de enviar un procedimiento legal con una dirección IP como identificador, Apple solicita a las autoridades competentes que determinen que la dirección IP del sujeto no es una dirección IP pública o de un router y que no utiliza la traducción de direcciones de red de nivel de operador (CGNAT) y que confirme a Apple, durante la notificación del procedimiento legal, que es una dirección IP no pública. Además, estas solicitudes deben incluir una restricción de fecha de no más de tres días. En respuesta a una solicitud de este tipo, Apple puede generar registros de conexión (consulte la sección III. Q más abajo) a partir de los cuales las autoridades pueden intentar identificar una cuenta o ID de Apple concretos para usarlos como identificador en una solicitud de procedimiento legal de seguimiento. Los datos de los clientes de Apple basados en una dirección IP, si están disponibles, se pueden obtener con la petición legalmente válida adecuada para el país del solicitante.

## **M. Otra información disponible sobre dispositivos**

**Dirección MAC:** la dirección de control de acceso al medio (dirección MAC, por sus siglas en inglés) es un identificador único asignado a interfaces de red para las comunicaciones en el segmento de red física. Cualquier producto de Apple con interfaces de red tendrá una o varias direcciones MAC, como Bluetooth, Ethernet, wifi o FireWire. La información sobre la dirección MAC, si está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante en la que se proporcione a Apple un número de serie (o el número IMEI, MEID o UDID en el caso de los dispositivos iOS).

## **N. Peticiones de los datos de videovigilancia de un Apple Store**

Los datos de videovigilancia pueden variar en función de la ubicación de la tienda. Estos datos



normalmente se conservan en un Apple Store durante un periodo máximo de 30 días. En muchas jurisdicciones, se guardan solo durante 24 horas en cumplimiento de las leyes locales. Una vez transcurrido este tiempo, los datos podrían no estar disponibles. Las peticiones de solo datos de videovigilancia pueden enviarse a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). El organismo gubernamental o la autoridad competente deben proporcionar la fecha, la hora y la información adicional de la transacción correspondientes a los datos solicitados.

## **O. Game Center**

Game Center es una red social de juegos de Apple. Es posible tener acceso a información sobre las conexiones a Game Center de un cliente o dispositivo. Si los registros de conexión están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **P. Activación de dispositivos iOS**

Cuando un cliente activa un dispositivo iOS con un operador de telefonía móvil o actualiza el software, Apple recibe cierta información del proveedor del servicio o del dispositivo, en función del evento. Las direcciones IP del evento, los números ICCID y otros identificadores del dispositivo pueden estar disponibles. Si esta información está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

**Doble SIM:** para dispositivos con doble SIM, la información del operador de la nano-SIM y/o eSIM, si está disponible, puede obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Una eSIM es una SIM digital que permite a los clientes activar un plan de datos de un operador sin necesidad de usar una nano-SIM física. Encontrará más información en [support.apple.com/es-es/HT209044](https://support.apple.com/es-es/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 cuentan con doble SIM con dos tarjetas nano-SIM.

## **Q. Registros de conexión**

Si está disponible, la actividad de conexión de un cliente o dispositivo a servicios de Apple como Apple Music, la app Apple TV, Apple Podcasts, Apple Books, iCloud, Mi ID de Apple y Foros de Discusión de Apple puede obtenerse de Apple. Estos registros de conexión con direcciones IP, si están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **R. Registros de Mi ID de Apple y iForgot**

Apple puede proporcionar los registros de Mi ID de Apple y iForgot vinculados a un cliente, que pueden incluir información sobre acciones de restablecimiento de la contraseña. Si los registros de conexión con direcciones IP están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **S. FaceTime**

Las comunicaciones de FaceTime están totalmente cifradas y Apple no tiene forma de descifrar estos datos cuando se encuentran en tránsito entre dispositivos. Apple no puede interceptar las comunicaciones de FaceTime. Apple tiene registros de invitaciones a llamadas de FaceTime cuando se

inicia una invitación de llamada de FaceTime. Estos registros no indican si la comunicación entre los clientes se ha producido realmente. Los registros de invitaciones a llamadas de FaceTime se conservan durante un máximo de 25 días. Los registros de invitaciones a llamadas de FaceTime, si están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **T. iMessage**

Las comunicaciones de iMessage están totalmente cifradas y Apple no tiene forma de descifrar estos datos cuando se encuentran en tránsito entre dispositivos. Apple no puede interceptar comunicaciones de iMessage ni tiene registros de comunicaciones de iMessage. Sin embargo, sí que dispone de registros de las consultas de compatibilidad con iMessage. Estos registros indican que la aplicación de un dispositivo (como Mensajes, Contactos o Teléfono, por ejemplo) ha iniciado una consulta dirigida a los servidores de Apple para determinar si un controlador de búsqueda (que puede ser un número de teléfono, una dirección de correo electrónico o un ID de Apple) es «compatible con iMessage», pero no indican si la comunicación entre los clientes se ha producido realmente. Apple no puede determinar si las comunicaciones de iMessage realmente han tenido lugar basándose en los registros de las consultas de compatibilidad con iMessage, ni puede identificar qué aplicación inició la consulta. Asimismo, los registros de las consultas de compatibilidad no confirman que realmente se intentara llevar a cabo una acción de iMessage. Estos registros se conservan durante 25 días como máximo. Si están disponibles, los registros de las consultas de compatibilidad con iMessage pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

## **U. App Apple TV**

Con la app Apple TV, los clientes pueden buscar, comprar, reproducir y suscribirse a programas de televisión y películas de Apple TV+, canales de Apple TV y apps y servicios de terceros. El historial de compras y descargas puede estar disponible.

Las peticiones de datos de clientes de la app Apple TV deben incluir el identificador del dispositivo (número de serie, IMEI, MEID o GUID) o el ID de Apple o la dirección de correo electrónico de la cuenta correspondiente. En caso de no disponer del ID de Apple o la dirección de correo electrónico de la cuenta, será necesario proporcionar a Apple los datos del cliente, ya sean su nombre completo y su número de teléfono o su nombre completo y su dirección física, para poder identificar la cuenta del cliente en cuestión. Los agentes del organismo gubernamental o la autoridad competente también deberán proporcionar un número de pedido de Apple válido o el número completo de la tarjeta de débito o crédito asociada a las compras en la app Apple TV. También podrá facilitarse el nombre de un cliente en combinación con estos parámetros, pero el nombre del cliente por sí solo no es suficiente para obtener información.

**Nota:** Por motivos de seguridad de los datos, si su petición legal contiene datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento protegido por contraseña o cifrado (PDF y en formato editable, como Numbers, Excel, Pages o Word) a [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Además, la contraseña deberá enviarse en un correo electrónico por separado. Asimismo, de acuerdo con las normas de seguridad del sistema, Apple no descargará documentos de peticiones legales mediante un enlace proporcionado en un correo electrónico.

## **V. Iniciar sesión con Apple**

Iniciar sesión con Apple es una manera que ofrece mayor privacidad a los clientes para registrarse en apps y sitios web de terceros con su ID de Apple actual. Un botón de Iniciar sesión con Apple en una

app o sitio web participante permite que el cliente pueda configurar una cuenta e iniciar sesión con su ID de Apple. En lugar de usar la cuenta de una red social o rellenar formularios y seleccionar otra contraseña, el cliente solo tiene que tocar el botón Iniciar sesión con Apple, revisar su información e iniciar sesión rápidamente de manera rápida y segura con Face ID, Touch ID o el código de su dispositivo. Encontrará más información en [support.apple.com/es-es/HT210318](https://support.apple.com/es-es/HT210318).

Ocultar mi correo electrónico es una prestación Iniciar sesión con Apple. Usa el servicio de relay 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. Es posible obtener información básica del cliente mediante una petición legalmente válida adecuada para el país del solicitante.

## IV.Preguntas frecuentes

**P: ¿Puedo enviar un correo electrónico a Apple para cuestiones relacionadas con una petición de información que yo mismo, en tanto que autoridad competente, haya realizado?**

R: Sí, es posible enviar preguntas o consultas acerca del proceso legal iniciado por el organismo gubernamental o autoridad competente por correo electrónico [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

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

R: No, no es necesario registrar un dispositivo en Apple para que funcione ni para poder usarlo.

**P: ¿Apple puede proporcionarme el código de un dispositivo iOS bloqueado?**

R: No, Apple no tiene acceso a las contraseñas de los usuarios.

**P: ¿Puedo recibir ayuda de Apple para devolver un dispositivo perdido o robado a la persona que lo perdió?**

R: En estos casos, póngase en contacto con [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Incluya el número de serie del dispositivo (o IMEI, en su caso) en el correo electrónico, junto con cualquier otra información relevante. La información sobre cómo encontrar el número de serie está disponible aquí: [support.apple.com/es-es/HT204308](https://support.apple.com/es-es/HT204308).

Si hay información del cliente disponible, Apple se pondrá en contacto con él y le dará información para ponerse en contacto con la autoridad competente para recuperar el dispositivo. Sin embargo, si no se puede determinar el cliente a partir de la información disponible, puede que se le indique que envíe una petición legal válida.

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

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

**P: ¿Qué se debe hacer con la información proporcionada a autoridades competentes una vez que la investigación o el caso penal hayan concluido?**

R: Todos los datos e información proporcionados a organismos gubernamentales o autoridades competentes con información de identificación personal (incluida cualquier copia realizada) deben destruirse una vez terminada la investigación, el caso penal y todas las apelaciones.

**P: ¿Apple notifica a los clientes que ha recibido peticiones de información de autoridades competentes en relación con su persona?**

R: Sí, la política de Apple en cuanto a notificaciones se aplica a las peticiones sobre cuentas por parte de autoridades competentes, organismos gubernamentales y entidades privadas. Apple notificará a sus clientes y titulares de cuentas a menos que haya una orden de información reservada o una orden de no revelación según la legislación aplicable, o cuando Apple considere, a su entera discreción, que la notificación puede poner en riesgo de lesión o muerte a un miembro del público, el caso esté relacionado con situaciones de peligro para un menor, o cuando la notificación no sea aplicable a las circunstancias del caso.