



Directrices para procesos legales

Organismos gubernamentales y autoridades competentes de fuera de Estados Unidos

Estas directrices están dirigidas a los organismos gubernamentales y las autoridades competentes de fuera de Estados Unidos que quieran solicitar información sobre los usuarios de dispositivos, productos y servicios de Apple a las entidades pertinentes de Apple que prestan servicio en la región o el país correspondiente. Apple actualizará las presentes directrices cuando sea necesario.

En estas directrices, Apple debe entenderse como la entidad pertinente responsable de la información de los clientes o usuarios en una región o un país en concreto. Apple, como empresa multinacional, tiene ubicadas en varias jurisdicciones una serie de entidades jurídicas que se responsabilizan de la información personal que recopilan y que Apple Inc. procesa en su nombre. Por ejemplo, la información de puntos de venta correspondiente a las entidades de Retail de fuera de Estados Unidos la controlan las entidades de Retail de Apple específicas de cada país. Es posible que estas entidades jurídicas ubicadas fuera de Estados Unidos también controlen la información personal relacionada con el Apple Online Store y iTunes, 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 usuarios relacionados con los servicios que Apple ofrece en las regiones a las que pertenecen.

Todas las demás peticiones de información relacionadas con clientes o usuarios de Apple, incluidas las preguntas de los clientes o usuarios acerca de la divulgación de información, deben remitirse a <https://www.apple.com/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 legislación estadounidense en materia de privacidad de las comunicaciones electrónicas (ECPA), excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Las peticiones en virtud de un Tratado de Asistencia Legal Mutua o un acuerdo con Estados Unidos se consideran conformes a la ECPA.

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 usuarios y proporciona la información cuando la ley así lo exige.

Apple cuenta con un proceso centralizado de recepción, seguimiento, procesamiento y respuesta para las peticiones legales válidas hechas por organismos gubernamentales, autoridades competentes y entidades privadas que abarca desde el momento en el que se reciben las peticiones hasta que se proporciona una respuesta. Un equipo cualificado de nuestro Departamento Jurídico se encarga de revisar y evaluar todas las peticiones recibidas. Si Apple considera que una petición no

tiene base legal o bien que no está clara, no es apropiada o es demasiado amplia, dicha petición se recusa o rechaza.

INDEX

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/eliminación de cuenta
- F. Notificación a los usuarios

III. Información en posesión de Apple

- A. Registro de dispositivos
- B. Registros del servicio de atención al cliente
- C. iTunes
- D. Transacciones en un Apple Store
- E. Compras en el Apple Online Store
- F. Tarjetas regalo
- G. iCloud
- H. Buscar mi iPhone
- I. Extracción de datos de dispositivos iOS bloqueados con contraseña
- J. Otra información disponible sobre dispositivos
- K. Peticiones de los datos de videovigilancia de un Apple Store
- L. Game Center
- M. Activación de dispositivos iOS
- N. Registros de inicio de sesión
- O. Registros de Mi ID de Apple y iForgot
- P. FaceTime
- Q. iMessage

IV. Preguntas frecuentes

I. Información general

Apple diseña, fabrica y comercializa dispositivos multimedia y de comunicación móvil, ordenadores personales y reproductores de música digital portátiles. Además, vende un amplio abanico de software, servicios, periféricos y soluciones de red propios, así como contenido digital y aplicaciones de terceros. La oferta de productos y servicios de Apple incluye el Mac, el iPhone, el iPad, el iPod, el Apple TV, el Apple Watch, una selección de aplicaciones de software para particulares y profesionales, los sistemas operativos iOS y Mac OS X, iCloud y diferentes accesorios, servicios y opciones de soporte. Apple también vende y distribuye contenido digital y aplicaciones a través del iTunes Store, App Store, iBooks Store y Mac App Store. Apple guarda la información de los usuarios de conformidad con la [política de privacidad de Apple](#) y los [términos de servicio/términos y condiciones](#) aplicables a un servicio determinado. Apple se compromete a preservar la privacidad de los usuarios de productos y servicios Apple («usuarios de Apple»). Por este motivo, no revelará información sobre los usuarios 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 la sección Preguntas frecuentes de estas directrices se pretende proporcionar respuestas a algunas de las preguntas más comunes que Apple recibe. Ni las presentes directrices ni el apartado de preguntas frecuentes cubren todas las circunstancias que pueden darse.

Si tiene más preguntas, póngase en contacto con 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.

La mayoría de las peticiones de autoridades competentes que recibe Apple solicitan información sobre un dispositivo Apple o cliente determinado y los servicios que Apple proporciona 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 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 legislación estadounidense en materia de privacidad de las comunicaciones electrónicas (ECPA), excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Las peticiones en virtud de un Tratado de Asistencia Legal Mutua o un acuerdo con Estados Unidos se consideran conformes a la ECPA.

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 en cuestión. 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 transmitirla 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.

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. Si la petición contiene cinco identificadores o más, como números de serie/IMEI de dispositivo, varios ID de Apple, direcciones de correo electrónico o números de factura/pedido, dichos identificadores deben estar en formato editable. Estos identificadores normalmente son necesarios para buscar información relacionada con dispositivos, cuentas o transacciones financieras.

Apple considera que una petición de información por parte de una autoridad competente es legalmente válida cuando existe un fundamento jurídico preciso en virtud de la legislación del país en cuestión y se realiza en el marco de una actuación preventiva de buena fe o de una actuación de detección o investigación de delitos. He aquí algunos ejemplos de peticiones que Apple considera legalmente válidas y recibe internacionalmente: Production Orders (Australia y Canadá), Tribunal Orders (Nueva Zelanda), Requisition or Judicial Rogatory Letters (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 (Reino Unido), así como órdenes o peticiones de tribunales de otros países.

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

Apple examina detenidamente todas las peticiones procedentes de organismos gubernamentales, autoridades competentes y entidades privadas para comprobar que tienen una base legal válida y que cumplen con los requisitos correspondientes. Si Apple determina que una petición no tiene base legal o que no está clara, no es apropiada o es demasiado amplia, la recusará o rechazará dicha petición.

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 legislación estadounidense en materia de privacidad de las comunicaciones electrónicas (ECPA), excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Las peticiones en virtud de un Tratado de Asistencia Legal Mutua o un acuerdo con Estados Unidos se consideran

conformes 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 Apple Inc., a la dirección lawenforcement@apple.com.

Las peticiones de conservación deberán incluir el ID de Apple o la dirección de correo electrónico de la cuenta pertinente, o bien el nombre completo y el número de teléfono, o el nombre completo y la dirección física asociados a la cuenta de Apple. Cuando se haya recibido una petición de conservación, Apple Inc. conservará durante 90 días un único registro de los datos del usuario 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. La recepción de más de dos peticiones de conservación para la misma cuenta se entenderá como una petición de ampliación del plazo de conservación de los materiales conservados inicialmente, pero Apple Inc. no conservará nuevos materiales en respuesta a dichas peticiones.

D. Peticiones de urgencia

Apple considera que una petición tiene carácter urgente cuando hace referencia a una circunstancia que constituye una amenaza seria e inminente para:

- 1) la vida o la seguridad de las personas;
- 2) la seguridad de un estado;
- 3) la seguridad de infraestructuras/instalaciones importantes.

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

Para enviar una petición de urgencia a Apple, el agente del organismo gubernamental o la autoridad competente debe rellenar la plantilla «[Petición de urgencia de información de autoridades competentes](#)» y enviarla directamente desde su dirección de correo electrónico oficial del organismo gubernamental o la autoridad competente a la dirección: exigent@apple.com, con las palabras «Emergency Request» en el asunto.

En caso de que Apple extraiga los datos del cliente en respuesta a una petición de información de urgencia por parte de un organismo gubernamental o autoridad competente, Apple podrá ponerse en contacto con un supervisor del agente del organismo gubernamental o la autoridad competente que envió dicha petición para confirmar que se trata de una petición de información urgente legítima. El agente del organismo gubernamental o la autoridad competente que envíe la petición de información debe proporcionar la información de contacto del supervisor en dicha petición.

Si el organismo gubernamental o la autoridad competente necesitan contactar con Apple en relación con una petición de urgencia fuera del horario establecido (antes de las 8:00 h o después de las 17:00 h de la hora del Pacífico), puede hacerlo llamando a Global Security Operations Center (GSOC) de Apple al 001 408 974-2095. En este número de teléfono se ofrece atención en distintos idiomas.

E. Peticiones de restricción/eliminación de cuenta

En el caso de que un organismo gubernamental o una autoridad competente quieran solicitar 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 (como una condena o resolución judicial) que demuestre que la cuenta que debe restringirse o eliminarse se ha utilizado ilegítimamente. Apple no procederá a restringir ni eliminar la cuenta de un cliente si la petición no es oficial o válida.

Apple examina detenidamente todas las peticiones procedentes de organismos gubernamentales y autoridades competentes para comprobar que se fundamentan en una base legal válida. Si Apple determina que una petición no tiene base legal o si la orden judicial no demuestra que la cuenta que debe restringirse o eliminarse se ha utilizado ilegítimamente, se recusará o rechazará dicha petición.

Si Apple recibe una orden judicial u otro procedimiento legal equivalente del país correspondiente (como una condena 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, se realizará la acción requerida para restringir o eliminar la cuenta conforme a la orden judicial y se comunicará oportunamente al agente que envía la petición.

F. Notificación a los usuarios

Apple notificará a sus clientes o usuarios que ha recibido una petición de información con validez legal referente a su cuenta de Apple hecha 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 el caso esté relacionado con situaciones de peligro para un menor; cuando la notificación no sea aplicable a las circunstancias del caso, o cuando Apple considere que la notificación puede poner en riesgo de lesión o muerte a una persona o a un grupo de personas en concreto, o bien entorpecer el curso de la justicia o perjudicar a la administración de justicia.

Transcurridos 90 días, Apple notificará a posteriori la existencia de peticiones de urgencia, salvo si dicha notificación se prohíba explícitamente por orden judicial o según la legislación aplicable, si el caso está relacionado con situaciones de peligro para un menor o si Apple considera que la notificación puede poner en riesgo de lesión o muerte a una persona o un grupo de personas en concreto. Apple notificará a posteriori la existencia de peticiones una vez que haya vencido el plazo de información reservada estipulado en una orden judicial, salvo cuando el caso esté relacionado con situaciones de peligro para un menor, cuando la notificación no sea aplicable a las circunstancias del caso o cuando Apple considere que la notificación puede poner en riesgo de lesión o muerte a una persona o a un grupo de personas en concreto, o bien entorpecer el curso de la justicia o perjudicar a la administración de justicia.

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

III. Información en posesión de Apple

En este apartado se detallan los tipos generales de información de los que Apple puede disponer en el momento de la publicación de estas directrices.

A. Registro de dispositivos

Los clientes proporcionan a Apple información básica personal o de registro (como el nombre, la dirección postal, la dirección de correo electrónico y el número de teléfono) cuando registran un dispositivo Apple con un sistema operativo anterior a iOS 8 y Mac OS Sierra 10.12. Apple no verifica dicha información, por lo que puede ser inexacta o no reflejar la identidad del 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 Mac OS Sierra 10.12 y versiones posteriores, se recibe cuando un cliente asocia un dispositivo a un ID de Apple vinculado a iCloud. Esta información puede ser inexacta o no reflejar la identidad del 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.

B. Registros del servicio de atención al cliente

Pueden obtenerse de Apple 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. iTunes

iTunes es una aplicación de software gratuita que los clientes utilizan para organizar y reproducir música y vídeos digitales en sus ordenadores. También es una tienda que permite a los clientes descargar contenido en sus ordenadores y dispositivos iOS. Cuando un cliente abre una cuenta de iTunes, puede proporcionar información de suscripción básica, como su nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, podemos disponer de información sobre conexiones para realizar transacciones de compra o descarga en iTunes, conexiones para obtener actualizaciones o nuevas descargas y conexiones a iTunes Match. Si la información de suscripción a iTunes y los registros de conexión con direcciones IP están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

Las peticiones de datos de iTunes deben incluir el identificador del dispositivo Apple (número de serie, IMEI, MEID o GUID), o bien 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 suscriptor de iTunes, ya sean su nombre completo y su

número de teléfono o su nombre completo y su dirección física, para poder identificar la cuenta de Apple asociada. Los agentes del organismo gubernamental o la autoridad competente también pueden proporcionar un número de pedido de iTunes válido o el número completo de una tarjeta de débito o crédito asociada a las compras de iTunes. Puede facilitarse un nombre de cliente junto con estos parámetros. Sin embargo, no es posible acceder a la información solo con el nombre del cliente.

Nota: Por motivos de seguridad de los datos, cuando su solicitud legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento o archivo protegido por contraseña o cifrado a lawenforcement@apple.com, y la contraseña deberá enviarse en un correo electrónico aparte.

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 solicitud legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento o archivo protegido por contraseña o cifrado a lawenforcement@apple.com, y la contraseña deberá enviarse en un correo electrónico aparte.

E. Compras en el Apple Online Store

Apple dispone de información referente a las compras hechas en el Apple Online Store, incluidos el nombre del comprador, la dirección de envío, el número de teléfono, la dirección de correo electrónico, el producto o los productos comprados, el importe de la compra y la dirección IP desde la que se realizó la compra. Las peticiones de información sobre pedidos del Apple Online Store deben incluir el número completo de una tarjeta de débito o crédito o el número de pedido, de referencia o de serie del artículo comprado. Puede facilitarse un nombre de cliente junto con estos parámetros. Sin embargo, no es posible acceder a la información solo con el nombre del cliente. Las peticiones de información sobre pedidos del Apple Online Store 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 o la dirección de correo electrónico de la cuenta, Apple requiere algunos datos del suscriptor, 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. Si la información sobre la compra en el Apple Online Store está disponible, puede obtenerse mediante una petición legalmente válida del país del solicitante.

Nota: Por motivos de seguridad de los datos, cuando su solicitud legal contenga datos completos de la tarjeta de crédito o débito, estos datos deberán enviarse en un documento o archivo protegido por contraseña o cifrado a lawenforcement@apple.com, y la contraseña deberá enviarse en un correo electrónico aparte.

F. Tarjetas regalo

Las tarjetas regalo del Apple Store y el iTunes Store cuentan con un número de serie y un código PIN (también conocido como código PIN de canje). El número de serie de estas tarjetas puede tener formatos distintos en función de variables como el diseño o la fecha de emisión. Los códigos PIN de canje de las tarjetas permiten usar el saldo que contienen. Estos códigos son el parámetro más fiable para que Apple busque información relacionada con las tarjetas regalo. En los casos en los que una petición legal incluya 5 o más códigos PIN de tarjetas regalo, Apple solicita que dichos códigos PIN se envíen también en formato electrónico editable.

i. Tarjetas regalo del Apple Store

Las tarjetas regalo del Apple Store pueden usarse para comprar artículos en el Apple Online Store o en un Apple Store. El código PIN de estas tarjetas empieza por la letra «Y». A veces, las tarjetas regalo del Apple Store más antiguas tienen un código PIN de 8 dígitos. Los registros disponibles pueden incluir información del comprador de la tarjeta regalo (si se ha comprado a Apple y no a un tercero), transacciones de compra asociadas y artículos comprados. En algunas ocasiones, es posible que Apple pueda cancelar o anular 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, cuando su solicitud legal contenga datos completos de una tarjeta regalo del Apple Store, estos datos deberán enviarse en un documento o archivo protegido por contraseña o cifrado a lawenforcement@apple.com, y la contraseña deberá enviarse en un correo electrónico aparte.

ii. Tarjetas regalo de iTunes

Las tarjetas regalo del iTunes Store pueden usarse en el iTunes Store, App Store, iBooks Store y Mac App Store. El código PIN de estas tarjetas empieza por la letra «X». Con el código PIN, Apple puede averiguar si la tarjeta se ha activado (es decir, si se ha adquirido en una tienda) o se ha canjeado (el saldo se ha añadido al crédito de una cuenta de iTunes).

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

Nota: Por motivos de seguridad de los datos, cuando su solicitud legal contenga datos completos de una tarjeta regalo del iTunes Store, estos datos deberán enviarse en un documento o archivo protegido por contraseña o cifrado a lawenforcement@apple.com, y la contraseña deberá enviarse en un correo electrónico aparte.

G. iCloud

iCloud es el servicio en la nube de Apple que permite a los usuarios acceder a su música, sus fotos, sus documentos y muchos otros contenidos desde todos sus dispositivos. iCloud también permite a los suscriptores realizar copias de seguridad de sus dispositivos iOS en este servicio. Con el servicio iCloud, los suscriptores 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. Cuando se utilizan proveedores externos para almacenar datos, Apple nunca les da las claves. Apple conserva las claves de cifrado en sus centros de datos de Estados Unidos.

iCloud es un servicio por suscripción. 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 suscriptor, 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.

Es posible obtener la información siguiente de iCloud:

i. Información de suscripción

Cuando un cliente configura una cuenta de iCloud, puede proporcionar a Apple información de suscripción básica, como su nombre, dirección física, dirección de correo electrónico y número de teléfono. Además, también puede estar disponible información sobre conexiones de funciones de iCloud. Si la información de suscripción a iCloud y los registros de conexión con direcciones IP están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante. Los registros de conexiones se conservan como máximo durante 30 días.

ii. Registros de correo

Los registros de correo de iCloud 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. Estos registros se conservan como máximo durante 30 días y, si están disponibles, pueden obtenerse mediante la petición legalmente válida adecuada para el país del solicitante.

iii. 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 suscriptor ha decidido mantener en la cuenta mientras está activa. Apple no conserva los contenidos eliminados una vez que se han 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 aplicaciones, iMessage, Business Chat, mensajes SMS y MMS y mensajes de voz. Todos los datos de contenido de iCloud almacenados por Apple se cifran en la ubicación del servidor. Cuando se utilizan proveedores externos para almacenar datos, Apple nunca les da las claves. Apple conserva las claves de cifrado en sus centros de datos de Estados Unidos.

Todas las peticiones de organismos gubernamentales y autoridades competentes de fuera de Estados Unidos sobre contenidos deben cumplir con la legislación correspondiente, incluida la legislación estadounidense en materia de privacidad de las comunicaciones electrónicas (ECPA), excepto en casos de urgencia (definidos en el apartado «Peticiones de urgencia»). Las peticiones en virtud de un Tratado de Asistencia Legal Mutua o un acuerdo con Estados Unidos se consideran conformes a la ECPA. Apple Inc. solo proporcionará los contenidos del suscriptor tal y como aparecen en su cuenta en respuesta a un proceso legalmente válido de este tipo.

H. Buscar mi iPhone

Buscar mi iPhone es una prestación que pueden activar los usuarios y que permite a los suscriptores de iCloud localizar su iPhone, iPad, iPod touch, Apple Watch o Mac 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. Hay más información sobre este servicio en <http://www.apple.com/icloud/find-my-iphone.html>.

Para que un usuario que ha perdido su dispositivo pueda usar Buscar mi iPhone, debe haber habilitado esta prestación en el dispositivo antes de perderlo. Esta prestación 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 ubicación de un dispositivo localizado con la prestación Buscar mi iPhone se proporciona únicamente al usuario, y Apple no dispone de los contenidos de los mapas ni de las alertas facilitados a través de este servicio. En el enlace de soporte siguiente se ofrece información y los pasos que pueden seguir los usuarios si han perdido o les han robado su dispositivo iOS: <https://support.apple.com/es-es/HT201472>.

Los registros de conexión de Buscar mi iPhone están disponibles durante un periodo aproximado de 30 días y, de estar 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 mi iPhone 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.

I. Extracción de datos de dispositivos iOS bloqueados con contraseña

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 de iOS.

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.

J. 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, Wi-Fi o FireWire. Esta información, 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).

K. 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 que son exclusivamente por datos de videovigilancia pueden enviarse a la dirección: lossprevention@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.

L. 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 usuario o dispositivo. Si están disponibles, los registros de conexión con direcciones IP y los registros de transacciones pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

M. Activación de dispositivos iOS

Cuando un cliente activa un dispositivo iOS 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 con una citación o un proceso legal más amplio. Una eSIM es una

SIM digital que permite a los usuarios activar un plan de datos de un operador sin necesidad de usar una Nano SIM física. Puede encontrar más información en <https://support.apple.com/es-es/HT209044>.

N. Registros de inicio de sesión

Apple puede facilitar información sobre la actividad de inicio de sesión de un usuario o dispositivo en servicios de Apple, como iTunes, iCloud, Mi ID de Apple y Foros de Discusión de Apple, siempre que esté disponible. Si los registros de conexión con direcciones IP están disponibles, pueden obtenerse mediante una petición legalmente válida adecuada para el país del solicitante.

O. Registros de Mi ID de Apple y iForgot

Apple puede proporcionar los registros de Mi ID de Apple y iForgot vinculados a un usuario, 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.

P. 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 llamadas de FaceTime cuando se inicia una invitación de llamada de FaceTime. Estos registros no indican si la comunicación entre los usuarios se ha producido realmente. Los registros de las invitaciones a llamadas FaceTime se guardan durante un máximo de 30 días. Si estos registros están disponibles, pueden obtenerse por orden judicial, por resolución judicial o mediante un equivalente del país en cuestión.

Q. 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 las comunicaciones de iMessage y no dispone de registros de dichas comunicaciones. 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 usuarios 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 30 días como máximo y si están disponibles, pueden obtenerse por orden judicial, por resolución judicial o mediante un equivalente del país en cuestión.

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, las preguntas o peticiones relacionadas con un proceso legal de un organismo gubernamental pueden enviarse a 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 la contraseña de un dispositivo iOS bloqueado?

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

P.: ¿Me puede ayudar a devolver un dispositivo perdido o robado a la persona que lo perdió?

R.: En estos casos, póngase en contacto con lawenforcement@apple.com. Incluya el número de serie o IMEI del dispositivo y cualquier otra información relevante. Si disponemos de información del cliente, nos pondremos en contacto con el titular y le invitaremos a 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 que contengan información que permita identificar a una persona (incluida cualquier copia realizada) deben destruirse una vez terminada la investigación, el caso penal y todas las apelaciones.

P.: ¿Apple notifica a los usuarios 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 divulgación según la legislación aplicable, o cuando Apple considere 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, o bien entorpecer el curso de la justicia o perjudicar a la administración de justicia.