



Lineamientos de revisión de apps

Las apps están cambiando el mundo, enriqueciendo la vida de las personas y permitiendo a los desarrolladores como tú innovar como nunca antes. Como resultado, el App Store se convirtió en un ecosistema dinámico y emocionante para millones de desarrolladores y más de mil millones de usuarios. Tanto si eres desarrollador novel como si cuentas con un gran equipo de programadores experimentados, nos entusiasma que crees apps para nuestras plataformas y queremos ayudarte a entender nuestros lineamientos para que tengas la seguridad de que tu app aprobará rápidamente el proceso de revisión.

Febrero de 2026

Introducción	4
Antes de enviar la app	5
1. Seguridad	6
1.1 Contenido censurable	6
1.2 Contenido generado por el usuario	7
1.2.1 Contenido de creadores	7
1.3 Categoría Niños	8
1.4 🚫 Daño físico	8
1.5 🚫 Información para desarrolladores	9
1.6 🚫 Seguridad de los datos	9
1.7 Denuncia de actividad delictiva	10
2. Rendimiento	10
2.1 Integridad de la app	10
2.2 Pruebas beta	10
2.3 🚫 Metadatos precisos	10
2.4 Compatibilidad de hardware	13
2.5 Requisitos de software	14
3. Negocios	16
3.1 Pagos	17
3.1.1 Compras dentro de la app	17
3.1.1(a) Enlace a otros métodos de compra	18
3.1.2 Suscripciones	18
3.1.2(a) Usos permitidos	19
3.1.2(b) Actualizaciones y paso a versiones anteriores	20
3.1.2(c) Información de suscripción	20
3.1.3 Otros métodos de compra	20
3.1.3(a) Apps de lectura	20
3.1.3(b) Servicios multiplataforma	20
3.1.3(c) Servicios empresariales	21
3.1.3(d) Servicios de persona a persona	21
3.1.3(e) Productos y servicios fuera de la app	21
3.1.3(f) Apps independientes y gratuitas	21
3.1.3(g) Apps de administración de publicidad	21
3.1.4 Contenido específico del hardware	21
3.1.5 Criptomonedas	22
3.2 Otros asuntos relativos al modelo de negocio	22
3.2.1 Prácticas aceptables	22

3.2.2 Prácticas inaceptables	23
4. Diseño	24
4.1 Imitaciones	24
4.2 Funcionalidad mínima	25
4.2.7 Clientes de escritorio remoto	25
4.3 Spam	26
4.4 🚫 Extensiones	26
4.5 🚫 Sitios y servicios de Apple	27
4.6 Se omitió intencionalmente.	28
4.7 🚫 Miniapps, minijuegos, juegos de streaming, chatbots, plug-ins y emuladores de juegos	28
4.8 🚫 Servicios de inicio de sesión	29
4.9 🚫 Apple Pay	30
4.10 🚫 Monetización de las capacidades integradas	30
5. 🚫 Legal	30
5.1 🚫 Privacidad	31
5.1.1 🚫 Recopilación y almacenamiento de datos	31
5.1.2 🚫 Uso e intercambio de datos	32
5.1.3 🚫 Salud e investigación médica	33
5.1.4 Niños	34
5.1.5 🚫 Localización	35
5.2 Propiedad intelectual	35
5.3 Juegos, apuestas y loterías	36
5.4 🚫 Apps de VPN	36
5.5 🚫 Administración de dispositivos móviles	37
5.6 🚫 Código de conducta para desarrolladores	37
5.6.1 Reseñas del App Store	37
5.6.2 🚫 Identidad del desarrollador	38
5.6.3 Detección de fraude	38
5.6.4 Calidad de la app	38
Después del envío	38

Introducción

El principio rector del App Store es simple: queremos ofrecer a los usuarios una experiencia segura a la hora de adquirir apps y una gran oportunidad de éxito a todos los desarrolladores. Para ello, ofrecemos un App Store muy selectivo en el que el equipo especializado revisa cada app y un equipo editorial ayuda a los usuarios a descubrir nuevas apps todos los días. También analizamos cada app en busca de malware y otro software que pueda afectar la seguridad y la privacidad del usuario. Estas iniciativas hicieron que las plataformas de Apple sean las más seguras para los consumidores de todo el mundo.

En la Unión Europea, los desarrolladores también pueden distribuir apps de iOS y iPadOS certificadas desde mercados de apps alternativos y directamente desde su sitio web. En Japón, los desarrolladores también pueden distribuir apps de iOS desde mercados de apps alternativos. Obtén más información sobre [mercados de apps alternativos](#), [distribución web](#) y [notarización para apps de iOS y iPadOS](#). Para ver qué lineamientos se aplican a la notarización para apps de iOS y iPadOS, haz clic en "Mostrar solo lineamientos de revisión de notarización" en el menú de la izquierda.

Para todo lo demás siempre está Internet. Si el modelo y los lineamientos del App Store o las distribuciones alternativas y la notarización para apps de iOS y iPadOS no se adaptan a tu app o idea de negocio, también ofrecemos Safari para brindarte una excelente experiencia web.

En las siguientes páginas, encontrarás nuestros lineamientos más recientes organizados en cinco secciones claras: Seguridad, Rendimiento, Negocios, Diseño y Legal. El App Store siempre está en constante cambio y mejora para ajustarse a las necesidades de nuestros clientes y productos. Tus apps también deberían cambiar y mejorar para permanecer en el App Store.

A continuación, te indicamos otros puntos que debes tener en cuenta a la hora de distribuir tu app en nuestras plataformas:

- Hay muchos niños que descargan un sinnúmero de apps. Los controles parentales funcionan muy bien para proteger a los niños, pero tú también debes hacer tu aporte. Así que no olvides tener en cuenta a los niños.
- El App Store es una excelente manera de llegar a cientos de millones de personas en todo el mundo. Si creas una app que solo quieres mostrarles a familiares y amigos, el App Store no es la mejor vía para hacerlo. Analiza la posibilidad de usar Xcode para instalar tu app en un dispositivo de forma gratuita o usa la distribución ad hoc disponible para los miembros de Apple Developer Program. Si eres principiante, obtén más información sobre [Apple Developer Program](#).
- Apoyamos firmemente que todos los puntos de vista estén representados en el App Store, siempre que las apps sean respetuosas con los usuarios con opiniones diferentes y la calidad de la experiencia con la app sea excelente. Rechazaremos las apps cuyo contenido o actividad creamos que esté fuera de lugar. Te preguntarán qué significa "fuera de lugar". Bueno, como dijo una vez un juez de la Corte Suprema: "Lo sabré cuando lo vea". Creemos que también lo sabrás tú cuando pases esa línea.
- Si intentas engañar al sistema (por ejemplo, si intentas burlar el proceso de revisión, robar datos del usuario, copiar el trabajo de otro desarrollador, manipular las calificaciones o el descubrimiento de apps en el App Store), tus apps se eliminarán de la tienda y se te expulsará de Apple Developer Program.

- Eres responsable de garantizar que todo el contenido de tu app cumpla con estos lineamientos, incluidas las redes de anuncios, los servicios de análisis y los kits de desarrollo de software (SDK) de terceros, por lo que debes revisarlos y seleccionarlos con sumo cuidado.
- Algunas funcionalidades y tecnologías que generalmente no están disponibles para los desarrolladores pueden ofrecerse como un derecho para casos de uso limitados. Por ejemplo, ofrecemos derechos para CarPlay Audio, HyperVisor y Privileged File Operations.

Esperamos que estos lineamientos te resulten útiles para transitar el proceso de revisión y que las aprobaciones y los rechazos se apliquen con coherencia en todos los casos. Este documento es dinámico: futuras apps pueden plantear nuevas cuestiones que ameriten la creación de nuevas reglas en cualquier momento. Tu app podría ser una de ellas. Nos encanta cuando esto sucede y reconocemos el valor de tu trabajo. Nuestro esfuerzo se centra en crear la mejor plataforma del mundo para que expreses tu talento y puedas vivir de él.

Antes de enviar la app

Para que la aprobación de tu app sea lo más fácil posible, revisa los errores comunes que se enumeran a continuación y que pueden ralentizar el proceso de revisión o provocar un rechazo. Esto no reemplaza los lineamientos ni garantiza la aprobación, pero asegurarse de poder verificar todos los elementos de la lista es un buen comienzo. Si la app ya no funciona como debería o dejas de mantenerla de forma activa, se eliminará del App Store. [Obtén más información sobre las mejoras del App Store](#).

Asegúrate de hacer lo siguiente:

- Prueba tu app para detectar fallas y errores.
- Asegúrate de que toda la información y los metadatos de la app estén completos y sean precisos.
- Actualiza tu información de contacto en caso de que App Review necesite comunicarse contigo.
- Proporciona a App Review acceso completo a tu app. Si tu app incluye funcionalidades basadas en la cuenta, proporciona una cuenta de demostración activa o un modo de demostración con todas las funcionalidades, además de cualquier otro hardware o recurso que pueda ser necesario para revisar tu app (p. ej., credenciales de inicio de sesión o un código QR de muestra).
- Habilita los servicios de back-end para que estén activos y accesibles durante la revisión.
- Incluye explicaciones detalladas de las funcionalidades no evidentes y las compras dentro de la app en las notas de App Review e incluye documentación complementaria cuando corresponda.
- Comprueba si tu app sigue las instrucciones de otros lineamientos, como los siguientes:

Documentación para desarrolladores

 [SwiftUI](#)

 [UIKit](#)

 [AppKit](#)

- [📄 Extensiones de apps](#)
- [📄 Optimización de datos de apps para el Respaldo en iCloud](#)
- [📄 Apple File System](#)
- [📄 Ayuda de App Store Connect](#)
- [📄 Ayuda para cuenta de desarrollador](#)

Lineamientos de diseño

- [📄 Human Interface Guidelines](#)

Lineamientos de marca y marketing

- [📄 Recursos de marketing y lineamientos de identidad](#)
- [📄 Lineamientos de marketing de Apple Pay](#)
- [📄 Lineamientos de Agregar a Apple Wallet](#)
- [📄 Lineamientos para el uso de las marcas comerciales y los derechos de autor de Apple](#)

Las lineamientos marcados con  se aplican a la [notarización para apps de iOS y iPadOS](#) en la UE y a la notarización para apps de iOS en Japón.

1. Seguridad

Cuando las personas instalan una app del App Store, quieren tener la certeza de que es seguro hacerlo, que la app no tiene contenido desagradable u ofensivo, que no dañará el dispositivo y que no es probable que su uso cause daños físicos. A continuación, describimos los principales obstáculos, pero si quieres conmocionar u ofender a las personas, el App Store no es el lugar adecuado para tu app. Algunas de estas reglas también se incluyen en la notarización para apps de iOS y iPadOS.

1.1 Contenido censurable

Las apps no deben incluir contenido ofensivo, desconsiderado, perturbador, desagradable, de mal gusto, o simplemente espeluznante. Entre los ejemplos de dicho contenido se incluyen los siguientes:

1.1.1 Contenido difamatorio, discriminatorio o malintencionado, como comentarios o referencias sobre religión, raza, orientación sexual, género, nacionalidad u origen étnico, u otros grupos específicos, sobre todo si la app puede humillar, intimidar o herir a personas o grupos específicos. Los humoristas y satíricos políticos profesionales generalmente están exentos de este requisito.

1.1.2 Representaciones realistas de personas o animales que son asesinados, mutilados, torturados o abusados, o contenido que fomenta la violencia. Los “enemigos” dentro del contexto de un juego no pueden apuntar únicamente a una raza, cultura, gobierno real, corporación en particular ni a ninguna otra entidad real.

1.1.3 Representaciones que fomenten el uso ilegal o imprudente de armas y objetos peligrosos, o que faciliten la compra de armas de fuego o municiones.

1.1.4 Material abiertamente sexual o pornográfico, definido como “descripciones o exhibiciones explícitas de órganos sexuales o actividades destinadas a estimular sentimientos eróticos en lugar de estéticos o emocionales”. Entre estas, se incluyen apps para “ligar” y otras apps que pueden incluir pornografía o usarse para facilitar la prostitución o la trata y la explotación de personas.

1.1.5 Comentarios religiosos provocativos o citas inexactas o engañosas de textos religiosos.

1.1.6 Información y funcionalidades falsas, incluidos datos del dispositivo inexactos o funcionalidades engañosas, como rastreadores de ubicación falsos. Indicar que la app es “para fines de entretenimiento” no es una excepción a este lineamiento. Se rechazarán las apps que permiten hacer llamadas telefónicas o enviar mensajes SMS/MMS anónimos o en broma.

1.1.7 Conceptos malintencionados que aprovechan eventos recientes o actuales, como conflictos violentos, ataques terroristas y epidemias, para obtener ganancias a partir de estos.

1.2 Contenido generado por el usuario

Las apps con contenido generado por el usuario presentan desafíos particulares, que van desde la infracción de la propiedad intelectual hasta el acoso anónimo. Para evitar el mal uso, las apps con contenido generado por el usuario o servicios de redes sociales deben incluir lo siguiente:

- Un método para filtrar el material censurable y evitar que se publique en la app.
- Un mecanismo para denunciar contenido ofensivo y dar respuestas oportunas a las inquietudes.
- La capacidad de bloquear a los usuarios que hacen uso indebido del servicio.
- Información de contacto publicada para que los usuarios puedan comunicarse contigo.

Las apps con contenido generado por el usuario y los servicios que terminen utilizándose principalmente para contenido pornográfico, experiencias del estilo Chatroulette, chats aleatorios o anónimos, cosificación de personas (por ejemplo, votaciones en las que se decide si una persona es atractiva o no) y que suponen amenazas físicas o acoso no se admiten en el App Store y se pueden eliminar sin previo aviso. Si tu app incluye contenido generado por el usuario desde un servicio web, se le permite mostrar ocasionalmente contenido no apropiado para el trabajo (NSFW) para adultos, siempre que el contenido se oculte de forma predeterminada y solo se muestre cuando el usuario lo active a través de tu sitio web.

1.2.1 Contenido de creadores

Las apps que incluyen contenido de una comunidad específica de usuarios llamados “creadores” son una gran oportunidad si se moderan adecuadamente. Estas apps presentan una experiencia única y unificada para que los clientes interactúen con varios tipos de contenido de creadores. Ofrecen herramientas y programas para que esta comunidad de creadores que no son desarrolladores cree, comparta y monetice las experiencias generadas por los usuarios. Estas experiencias no deben cambiar la funcionalidad y las características principales de la app nativa, sino que agregan contenido a esas

experiencias estructuradas. Estas experiencias no son “apps” nativas programadas por los desarrolladores, sino que representan el contenido de la propia app, y App Review las trata como contenido generado por el usuario. Entre el contenido de creadores, se pueden incluir videos, artículos, audio e incluso juegos informales. El App Store es compatible con las apps que ofrecen dicho contenido generado por el usuario, siempre y cuando sigan todos los lineamientos, incluido el lineamiento 1.2 sobre la moderación del contenido generado por el usuario y el lineamiento 3.1.1 sobre los pagos y las compras dentro de la app. Debes comunicarles a los usuarios qué contenido requiere compras adicionales.

(a) 🚫 Las apps para creadores deben proporcionar una manera para que los usuarios identifiquen el contenido que supera la clasificación por edad de la app y usar un mecanismo de restricción de edad basado en la edad verificada o declarada para limitar el acceso de los usuarios menores de edad.

1.3 Categoría Niños

La categoría Niños es una excelente manera para que las personas encuentren fácilmente apps diseñadas para niños. Si quieres participar en la categoría Niños, debes enfocarte en crear una gran experiencia específicamente para los usuarios más jóvenes. Estas apps no deben incluir enlaces fuera de la app, oportunidades de compra u otras distracciones para los niños, a menos que estén reservadas para un área designada detrás de un filtro de control parental. Ten en cuenta que una vez que los clientes confían en que tu app cumple con los requisitos de la categoría Niños, la app deberá seguir cumpliendo con estos lineamientos en las actualizaciones posteriores, incluso si decides anular la selección de la categoría. Obtén más información sobre los [filtros de control parental](#).

Debes cumplir con las leyes de privacidad relacionadas con la recopilación de datos de niños en línea que rigen en todo el mundo. Asegúrate de consultar la [sección sobre privacidad](#) de estos lineamientos para obtener más información. Además, las apps de la categoría Niños no pueden enviar información de identificación personal o información del dispositivo a terceros. Las apps de la categoría Niños no deben incluir análisis ni publicidad de terceros. Esto brinda una experiencia más segura para los niños. En casos limitados, se pueden permitir análisis de terceros siempre que los servicios no recopilen ni transmitan el identificador para anunciantes (IDFA), ni ningún dato identificable sobre los niños (como el nombre, la fecha de nacimiento, la dirección de correo electrónico), su ubicación o sus dispositivos. Esta excepción rige para cualquier dispositivo, red u otra información que pueda usarse directamente o combinarse con otra información para identificar a los usuarios y sus dispositivos. La publicidad contextual de terceros también se puede permitir en casos limitados, siempre y cuando los servicios tengan prácticas y políticas documentadas públicamente para las apps de la categoría Niños que incluyan la revisión humana de los mensajes publicitarios para verificar su idoneidad para la edad.

1.4 🚫 Daño físico

Si tu app conlleva un riesgo de daño físico, es posible que la rechacemos. Por ejemplo:

1.4.1 🚫 Es posible que analicemos con mayor detenimiento las apps de atención médica que podrían proporcionar información o datos inexactos, o que podrían usarse para diagnosticar o tratar pacientes.

- Las apps deben indicar con claridad los datos y la metodología que se usa para respaldar las afirmaciones sobre la precisión de sus mediciones de salud. Si el nivel de precisión o la metodología no se pueden validar, rechazaremos tu app. Por ejemplo, no se permiten las apps que afirman tomar

radiografías, medir la presión arterial, la temperatura corporal, los niveles de glucosa en sangre o los niveles de oxígeno en sangre únicamente mediante los sensores del dispositivo.

- Las apps deben recordarles a los usuarios que deben consultar con un médico además de usar la app y antes de tomar decisiones médicas.

Si tu app de atención médica recibió autorización regulatoria, envía un enlace a esa documentación con tu app.

1.4.2 ➡ Las calculadoras de dosis de medicamentos deben proceder del fabricante del medicamento, un hospital, una universidad, una compañía de seguros médicos, una farmacia u otra entidad autorizada, o recibir la aprobación de la Administración de Alimentos y Medicamentos (FDA) de EE. UU. o de una de sus contrapartes internacionales. Dado el daño que puede suponer para los pacientes, debemos asegurarnos de que la app se mantendrá y se actualizará de forma debida a lo largo del tiempo.

1.4.3 No se permiten apps que fomenten el consumo de tabaco y productos de vapeo, drogas ilegales o cantidades excesivas de alcohol. Se rechazarán las apps que incentiven a los menores a consumir alguna de estas sustancias. No está permitido facilitar la venta de sustancias controladas (excepto en el caso de las farmacias autorizadas y los dispensarios de cannabis autorizados o legales) ni de tabaco.

1.4.4 ➡ Las apps solo pueden mostrar puntos de control de conducción en estado de ebriedad (DUI) publicados por las agencias policiales y nunca deben fomentar la conducción bajo los efectos del alcohol u otra conducta imprudente, como la conducción a velocidad excesiva.

1.4.5 ➡ Las apps no deben instar a los clientes a participar en actividades (como apuestas, desafíos, etc.) ni a usar sus dispositivos de forma que supongan un riesgo de daño físico para sí mismos o para las demás personas.

1.5 ➡ Información para desarrolladores

Las personas deben saber cómo comunicarse contigo en caso de dudas o problemas técnicos. Asegúrate de que tu app y su URL de soporte técnico ofrezcan una forma sencilla de ponerse en contacto contigo. Se trata de algo de especial importancia en el caso de las apps que pueden usarse en el aula. La omisión de información de contacto precisa y actualizada no solo puede ser frustrante para los clientes, sino que puede infringir la ley en algunos países o regiones. Además, asegúrate de que los pases de Wallet incluyan información de contacto válida de la entidad emisora y estén firmados con un certificado específico asignado al propietario de la marca o la marca comercial del pase.

1.6 ➡ Seguridad de los datos

Las apps deben implementar las medidas de seguridad adecuadas para garantizar el uso adecuado de la información del usuario recopilada de conformidad con el Acuerdo de licencia de Apple Developer Program y estos lineamientos (consulta el lineamiento 5.1 para obtener más información), así como prohibir el uso, la divulgación y el acceso de terceros sin autorización.

1.7 Denuncia de actividad delictiva

Las apps para denunciar una presunta actividad delictiva deben contar con la participación de las fuerzas de seguridad locales y solo pueden ofrecerse en países o regiones donde exista esa posibilidad de participación.

2. Rendimiento

2.1 Integridad de la app

(a) ➡ Las apps que envíes a App Review, incluidas las destinadas a preventa, deben ser versiones finales con todos los metadatos necesarios y las URL en perfecto funcionamiento. El texto de los marcadores de posición, los sitios web vacíos y cualquier otro contenido temporal deben eliminarse antes del envío. Asegúrate de que tu app se haya probado en el dispositivo para detectar errores y verificar su estabilidad antes de enviarla, e incluye información sobre la cuenta de demostración (y activa el servicio de back-end) si la app requiere un inicio de sesión. Si no puedes proporcionar ninguna cuenta de demostración debido a obligaciones legales o de seguridad, puedes incluir un modo de demostración integrado en lugar de una cuenta de demostración con la aprobación previa de Apple. Asegúrate de que en el modo de demostración se muestren todas las funcionalidades de la app. Rechazaremos los paquetes de apps incompletos y los archivos binarios que se bloqueen o presenten problemas técnicos evidentes.

(b) Si ofreces compras dentro de la app, asegúrate de que estén completas, actualizadas y visibles para el revisor, y que funcionen correctamente. Si no se puede encontrar o revisar algún artículo de compra dentro de la app configurado en la app, explica el motivo en las notas de revisión.

2.2 Pruebas beta

Las demostraciones y las versiones beta y de prueba de las apps no se admiten en el App Store. Para esos casos, debes usar TestFlight. Cualquier app enviada para distribución beta a través de TestFlight debe estar destinada a la distribución pública y debe cumplir con los lineamientos de revisión de apps. Sin embargo, ten en cuenta que las apps que usan TestFlight no se pueden distribuir a los evaluadores a cambio de una compensación de ningún tipo, ni siquiera como recompensa por el financiamiento colectivo. Las actualizaciones importantes de la versión beta deben enviarse a App Review de TestFlight antes de distribuirse a los evaluadores. Para obtener más información, visita la página sobre las [pruebas beta de TestFlight](#).

2.3 ➡ Metadatos precisos

Los clientes deben saber lo que obtienen cuando descargan o compran tu app, así que asegúrate de que todos los metadatos de la app, incluida la información de privacidad, la descripción de la app, las capturas de pantalla y las vistas previas reflejen con precisión la experiencia principal de la app, y recuerda mantenerlos actualizados con las nuevas versiones.

2.3.1

(a) ➡ No incluyas funcionalidades ocultas, inactivas o no documentadas en tu app: la funcionalidad de tu app debe ser clara para los usuarios finales y App Review. Todas las funcionalidades nuevas y los cambios del producto deben describirse con detalle en la sección de notas para revisión de App Store Connect (se rechazarán las descripciones genéricas) y deben estar disponibles para su revisión. Del mismo modo, promocionar la app de forma engañosa, al igual que promocionar contenido o servicios que realmente no ofrece (p. ej., escáneres de virus y malware basados en iOS) o promocionar un precio falso, ya sea dentro o fuera del App Store, es motivo para eliminar la app del App Store o bloquear la instalación a través de una distribución alternativa y cancelar la cuenta del desarrollador.

(b) Un mal comportamiento notorio o reiterado es motivo de expulsión de Apple Developer Program. Nos esforzamos para hacer del App Store un ecosistema confiable y esperamos que nuestros desarrolladores de apps hagan lo mismo. No queremos hacer negocios con personas deshonestas.

2.3.2 Si tu app incluye compras dentro de ella, asegúrate de que la descripción, las capturas de pantalla y las vistas previas de la app indiquen claramente si hay elementos destacados, niveles, suscripciones, etc. que requieren compras adicionales. Si decides promocionar compras dentro de la app en el App Store, asegúrate de que el nombre de visualización, la captura de pantalla y la descripción de dichas compras sean adecuadas para destinatarios públicos, que sigas los lineamientos establecidos en [Promoción de compras dentro de la app](#) y que tu app administre correctamente el [método SKPaymentTransactionObserver](#) para que los clientes puedan completar la compra sin problemas cuando lances la app.

2.3.3 En las capturas de pantalla se debe mostrar la app en uso y no solo el título, la página de inicio de sesión o la pantalla de bienvenida. También pueden incluir superposiciones de texto e imágenes (p. ej., para demostrar los mecanismos de entrada, como un punto táctil animado o el Apple Pencil) y mostrar una funcionalidad extendida en el dispositivo, como Touch Bar.

2.3.4 Las vistas previas son una excelente manera de que los clientes vean cómo se ve tu app y para qué sirve. Para garantizar que las personas comprendan lo que obtendrán con tu app, las vistas previas solo pueden emplear capturas de pantalla de videos de la app en sí. Los stickers y las extensiones de iMessage pueden mostrar la experiencia del usuario en la app Mensajes. Puedes agregar superposiciones de texto o narración y videos para explicar lo que no quede claro en el video.

2.3.5 ➡ Selecciona la categoría más apropiada para tu app y consulta las [Definiciones de categorías del App Store](#) si necesitas ayuda. Si te equivocaste de categoría, podemos cambiarla por ti.

2.3.6 ➡ Responde con sinceridad las preguntas de clasificación según la edad en App Store Connect para que tu app se ajuste correctamente a los controles parentales. Si tu app está mal clasificada, los clientes podrían sorprenderse con lo que obtienen, o se podría desencadenar una investigación por parte de los reguladores gubernamentales. Si tu app incluye contenido multimedia que requiere la visualización de clasificaciones de contenido o advertencias (p. ej., películas, música, juegos, etc.), eres responsable de cumplir con los requisitos locales en cada territorio donde tu app esté disponible.

2.3.7 🚫 Elige un nombre de app único, asigna palabras clave que describan con precisión tu app y no intentes incluir en los metadatos términos de marcas registradas, nombres de apps famosas, información sobre precios u otras frases irrelevantes solo para engañar al sistema. Los nombres de las apps deben tener un límite de 30 caracteres. Los metadatos, como los nombres, los subtítulos, las capturas de pantalla y las vistas previas de las apps, no deben incluir precios, términos o descripciones que no sean específicos del tipo de metadatos. Los subtítulos de la app son una excelente manera de proporcionar contexto adicional para la app. Deben seguir nuestras reglas de metadatos estándar y no deben incluir contenido inapropiado, hacer referencia a otras apps ni hacer afirmaciones no verificables sobre el producto. Apple puede modificar las palabras clave inapropiadas en cualquier momento o tomar otras medidas adecuadas para evitar el uso indebido.

2.3.8 🚫 Los metadatos deben ser apropiados para todos los destinatarios, por lo que debes asegurarte de que los íconos de las compras dentro de la app, las capturas de pantalla y las vistas previas de la app cumplan con una clasificación para mayores de 4 años, incluso si tu app tiene una clasificación más alta. Por ejemplo, si tu app es un juego que se caracteriza por la violencia, selecciona imágenes que no muestren una muerte espantosa o una pistola que apunta a un personaje concreto. El uso de términos como “Para niños” y “Para menores” en los metadatos de la app está reservado en el App Store para la categoría Niños. No olvides asegurarte de que los metadatos, como el nombre y los íconos de la app (pequeño, grande, app para el Apple Watch, íconos alternativos, etc.), sean similares para no generar confusión.

2.3.9 Eres responsable de garantizar los derechos de uso de todos los materiales de los íconos, las capturas de pantalla y las vistas previas de tu app, y debes mostrar información ficticia de la cuenta en lugar de datos de una persona real.

2.3.10 Asegúrate de que tu app se centre en la experiencia de las plataformas de Apple que admite y no incluyas nombres, íconos ni imágenes de otras plataformas móviles o mercados de apps alternativos en tu app o metadatos, a menos que exista una funcionalidad interactiva específica y aprobada. Asegúrate de que los metadatos de la app se centren en la app en sí y en su experiencia. No incluyas información irrelevante.

2.3.11 Las apps que envíes para preventa en el App Store deben estar listas y poder entregarse tal como se envían. Asegúrate de que la app que eventualmente lances no difiera de manera sustancial de lo que anuncies mientras la app se encuentra en la etapa de preventa. Si haces cambios importantes en la app (p. ej., si cambias los modelos de negocio), debes volver a iniciar las preventas.

2.3.12 En las apps se deben describir claramente las funcionalidades nuevas y los cambios de productos en la sección “Novedades”. Las correcciones de errores simples, las actualizaciones de seguridad y las mejoras de rendimiento pueden basarse en una descripción genérica, pero los cambios más importantes deben indicarse en las notas.

2.3.13 Los eventos dentro de la app son eventos puntuales que tienen lugar dentro de tu app. Para que un evento aparezca en el App Store, debe pertenecer a un tipo de evento proporcionado en App Store Connect. Todos los metadatos del evento deben ser precisos y referirse al evento en sí, no a la app en general. Los eventos deben celebrarse en las fechas y horas que selecciones en App Store Connect, incluso en diferentes tiendas. Puedes monetizar tu evento siempre que sigas las normas establecidas en la sección 3 sobre negocios. Además, el enlace profundo del evento debe dirigir a los usuarios al destino

adecuado dentro de tu app. Lee [Eventos dentro de la app](#) para obtener información detallada sobre los metadatos y enlaces profundos aceptables de los eventos.

2.4 Compatibilidad de hardware

2.4.1 Para garantizar que las personas aprovechen al máximo tu app, las apps del iPhone deben poder ejecutarse en el iPad siempre que sea posible. Te recomendamos que consideres crear apps que los clientes puedan usar en [todos sus dispositivos](#).

2.4.2  Diseña tu app para que optimice el uso de la batería y no ponga en riesgo el dispositivo. Las apps no deben agotar rápidamente la batería, generar calor excesivo ni sobrecargar innecesariamente los recursos del dispositivo. Por ejemplo, en las apps no se debe aconsejar colocar el dispositivo debajo de un colchón o una almohada durante la carga ni ejecutar ciclos de escritura excesivos en la unidad de estado sólido. Ni las apps ni los anuncios de terceros que aparecen en ellas pueden ejecutar en segundo plano procesos ajenos a su funcionalidad principal, como la minería de criptomonedas.

2.4.3 Las personas deberían poder usar la app Apple TV sin la necesidad de incorporar otro tipo de hardware aparte de Siri Remote o controladores de juegos de terceros, pero puedes ofrecer una funcionalidad mejorada cuando se conecten dispositivos periféricos. Si necesitas un controlador de juegos, asegúrate de explicarlo claramente en los metadatos para que los clientes sepan que necesitan equipos adicionales para jugar.

2.4.4  En las apps nunca se debe indicar ni exigir un reinicio del dispositivo o modificaciones en la configuración del sistema que no estén relacionadas con la funcionalidad principal de la app. Por ejemplo, no aconsejes a los usuarios desactivar el Wi-Fi, deshabilitar las funcionalidades de seguridad, etc.

2.4.5 Las apps distribuidas a través del Mac App Store tienen algunos requisitos adicionales que se deben tener en cuenta:

(i) Deben estar en una zona protegida adecuada y cumplir con la [Documentación del sistema de archivos de macOS](#). Además, solo deben usar las interfaces de programación de apps (API) de macOS adecuadas para modificar los datos de usuarios almacenados por otras apps (p. ej., marcadores, Agenda o entradas del Calendario).

(ii) Deben empaquetarse y enviarse con las tecnologías proporcionadas en Xcode. No se permiten instaladores de terceros. También deben ser paquetes de instalación de apps independientes y no pueden instalar código ni recursos en ubicaciones compartidas.

(iii) No pueden autoiniciarse ni hacer que otro código se ejecute automáticamente al iniciarse o iniciar sesión sin consentimiento, ni generar procesos que sigan ejecutándose sin consentimiento después de que el usuario haya salido de la app. No deben agregar automáticamente sus íconos al Dock ni dejar atajos en el escritorio del usuario.

(iv) No pueden descargar ni instalar apps independientes, extensiones de kernel, código adicional ni recursos para agregar funcionalidades o cambiar sustancialmente la app con respecto a lo que vemos durante el proceso de revisión.

- (v) No pueden solicitar la elevación a privilegios raíz ni usar atributos setuid.
- (vi) No pueden presentar una pantalla de licencia al abrirse, requerir claves de licencias ni implementar su propia protección contra copias.
- (vii) Deben usar el Mac App Store para distribuir actualizaciones. No se permiten otros mecanismos de actualización.
- (viii) Las apps deben ejecutarse en el sistema operativo actual y no pueden usar tecnologías obsoletas o de instalación opcional (p. ej., Java).
- (ix) Las apps deben contener todos los idiomas y localizaciones compatibles en un solo paquete de apps.

2.5 Requisitos de software

2.5.1 ➡ Las apps solo pueden usar API públicas y deben ejecutarse en el sistema operativo actual. Obtén más información sobre las [API públicas](#). Mantén las apps actualizadas y asegúrate de eliminar las funcionalidades, las tecnologías o los marcos obsoletos que ya no serán compatibles con las versiones futuras de un sistema operativo. Las apps deben usar API y marcos para los fines previstos e indicar esa integración en la descripción de la app. Por ejemplo, el marco de HomeKit debe proporcionar servicios de automatización del hogar. Además, HealthKit debe usarse con fines de salud y bienestar, e integrarse con la app Salud.

2.5.2 ➡ Las apps deben ser independientes en sus paquetes y no pueden leer ni escribir datos fuera del área de contenedor designada, y tampoco pueden descargar, instalar ni ejecutar código que introduzca o cambie características o funcionalidades de la app, incluidas otras apps. Las apps educativas diseñadas para enseñar, desarrollar o permitir que los estudiantes prueben el código ejecutable pueden, en circunstancias limitadas, descargar el código siempre que dicho código no se use para otros fines. Estas apps deben hacer que el usuario pueda ver y editar el código fuente proporcionado por la app.

2.5.3 ➡ Se rechazarán las apps que transmitan virus, archivos, códigos informáticos o programas que puedan dañar o interrumpir el funcionamiento normal del sistema operativo o las características del hardware, incluidas las notificaciones push y Game Center. Las infracciones graves y la reincidencia darán lugar a la expulsión de Apple Developer Program.

2.5.4 ➡ Las apps que permitan realizar varias tareas al mismo tiempo solo pueden usar servicios en segundo plano para los fines previstos: VoIP, reproducción de audio, ubicación, finalización de tareas, notificaciones locales, etc.

2.5.5 Las apps deben ser completamente funcionales en redes IPv6 exclusivas.

2.5.6 ➡ Las apps que permitan navegar por la web deben usar el marco de WebKit adecuado y JavaScript de WebKit. Puedes solicitar el derecho de usar un motor de navegación web alternativo en tu app. [Obtén más información sobre estos derechos](#).

2.5.7 Se omitió intencionalmente.

2.5.8 Se rechazarán las apps que creen entornos alternativos de escritorio o pantalla de inicio.

2.5.9 Se rechazarán las apps que alteren o desactiven las funciones de los botones estándar, como los controles de volumen y el interruptor de timbre, u otros elementos o comportamientos nativos de la interfaz de usuario. Por ejemplo, las apps no deben bloquear enlaces a otras apps u otras funcionalidades que los usuarios esperan que funcionen de cierta manera.

2.5.10 Se omitió intencionalmente.

2.5.11 🚫 SiriKit y Atajos

(i) Las apps que integran SiriKit y Atajos solo deben registrarse para los fines que puedan cumplir sin recurrir a otra app y que los usuarios esperarían de la funcionalidad indicada. Por ejemplo, si tu app es una app de planificación de comidas, no debes incorporar la intención de comenzar un entrenamiento, incluso si la app comparte la integración con una app de fitness.

(ii) Asegúrate de que el vocabulario y las frases de tu lista de propiedades sean las adecuadas para tu app y la funcionalidad de Siri respecto de los fines para los que se registró la app. Los alias deben relacionarse directamente con el nombre de tu app o empresa y no deben ser términos genéricos ni incluir nombres de apps o servicios de terceros.

(iii) Resuelve la solicitud de Siri o el Atajo de la manera más directa posible y no insertes anuncios ni otros tipos de publicidades entre la solicitud y su cumplimiento. Solo solicita una desambiguación cuando sea necesario para completar la tarea (p. ej., pedirle al usuario que especifique un tipo particular de entrenamiento).

2.5.12 🚫 Las apps que usen CallKit o que incluyan una extensión antifraude por SMS solo deben bloquear los números de teléfono que sean spam confirmado. Las apps que incluyen funcionalidades de bloqueo de llamadas, SMS y MMS o identificación de spam deben identificar claramente estas funcionalidades en su texto de marketing y explicar los criterios de sus listas de mensajes bloqueados y de spam. No puedes usar los datos a los que accedas a través de estas herramientas para ningún fin que no esté directamente relacionado con el funcionamiento o la mejora de tu app o extensión (p. ej., no podrás usarlos, compartirlos ni venderlos con fines de seguimiento, creación de perfiles de usuario, etc.).

2.5.13 🚫 Las apps que usen reconocimiento facial para la autenticación de la cuenta deben usar [LocalAuthentication](#) (y no ARKit u otra tecnología de reconocimiento facial) cuando sea posible y deben contar con un método de autenticación alternativo para los usuarios menores de 13 años.

2.5.14 🚫 Las apps deben solicitar el consentimiento explícito del usuario y proporcionar una indicación visual o auditiva clara al grabar o registrar de cualquier modo la actividad del usuario. Entre estos registros se incluye cualquier uso de la cámara del dispositivo, el micrófono, las grabaciones de pantalla o cualquier otra entrada de datos del usuario.

2.5.15 Las apps que permiten a los usuarios ver y seleccionar archivos deben incluir elementos de la app Archivos y los documentos de iCloud del usuario.

2.5.16 ➡ Los widgets, las extensiones y las notificaciones deben guardar relación con el contenido y la funcionalidad de tu app.

(a) Además, todas las funcionalidades y características de App Clip deben estar incluidas en el archivo binario principal de la app. Los App Clips no pueden contener publicidad.

2.5.17 ➡ Las apps que admiten Matter deben usar el marco de soporte de Apple para que Matter inicie el enlace. Además, si eliges usar cualquier componente de software de Matter en tu app que no sea el SDK de Matter proporcionado por Apple, el componente de software debe estar certificado por la [Connectivity Standards Alliance](#) correspondiente a la plataforma en la que se ejecute.

2.5.18 ➡ La publicidad gráfica debe limitarse al archivo binario principal de la app y no debe incluirse en extensiones, App Clips, widgets, notificaciones, teclados, apps de watchOS, etc. Los anuncios que se muestran en una app deben ser apropiados para la clasificación por edad de la app y permitir que el usuario vea toda la información usada para identificarlo como audiencia (sin que el usuario deba cerrar la app), y no pueden participar en ninguna publicidad dirigida o conductual basada en datos confidenciales del usuario, como datos de salud o médicos (p. ej., de las API de HealthKit), datos de la escuela y el aula (p. ej., de ClassKit), o datos de niños (p. ej., de apps de la categoría Niños del App Store), etc. Los anuncios intercalados o que interrumpan o bloqueen la experiencia del usuario deben indicar claramente que son anuncios, no deben manipular ni engañar a los usuarios para que los toquen y deben proporcionar botones visibles y de fácil acceso que sean lo suficientemente grandes como para que los usuarios puedan cerrarlos u omitirlos con facilidad. Las apps que contienen anuncios también deben incluir una opción para que los usuarios puedan denunciar anuncios inapropiados o inadecuados según la edad.

3. Negocios

Hay muchas formas de monetizar tu app en el App Store. Si tu modelo de negocio no es evidente, asegúrate de explicarlo en los metadatos y en las notas para App Review. Si no entendemos cómo funciona tu app o si las compras dentro de la app no son evidentes de inmediato, la revisión se demorará y puede que termine en rechazo. Además, si bien el precio lo determinas tú, no distribuiremos apps ni artículos para compras dentro de la app a precios claramente abusivos. Rechazaremos las apps costosas que intenten engañar a los usuarios con precios irracionalmente altos.

Si descubrimos que intentaste manipular las reseñas, inflar las clasificaciones de las listas con comentarios pagados, incentivados, filtrados o falsos, o contratar servicios de terceros para que lo hagan en tu nombre, tomaremos medidas para preservar la integridad del App Store, entre las que se puede considerar la expulsión de Apple Developer Program.

3.1 Pagos

3.1.1 Compras dentro de la app

- Si quieres activar funcionalidades dentro de tu app (p. ej., suscripciones, monedas de juegos, niveles de juego, acceso a contenido premium o activación de una versión completa), debes usar la funcionalidad de compra dentro de la app. Las apps no pueden usar sus propios mecanismos para activar contenido o funcionalidades, como claves de licencia, marcadores de realidad aumentada, códigos QR, criptomonedas y carteras de criptomonedas, etc.
- Las apps pueden usar monedas de compras dentro de la app para permitir que los clientes “dejen propina” al desarrollador o a los proveedores de contenido digital en la app.
- Los créditos o las monedas de juegos que se adquieran mediante compras dentro de la app no deben vencer, y debes asegurarte de tener un mecanismo de restauración para las compras dentro de la app que se puedan restaurar.
- Las apps pueden permitir regalar a otras personas artículos a través de compras dentro de la app. Dichos regalos solo se pueden reembolsar al comprador original y no se pueden intercambiar.
- Las apps distribuidas a través del Mac App Store pueden contener plug-ins o extensiones activados con mecanismos diferentes a los del App Store.
- Las apps que ofrecen “cajas de recompensas” u otros mecanismos que ofrecen artículos virtuales aleatorios para la compra deben indicar las probabilidades de recibir cada tipo de artículo a los clientes antes de la compra.
- Las tarjetas de regalo, los certificados, los vales y los cupones digitales que se pueden canjear por productos o servicios digitales solo se pueden vender en la app mediante compras dentro de la app. Las tarjetas de regalo físicas que se venden dentro de una app y luego se envían por correo a los clientes pueden usar métodos de pago distintos de los de las compras dentro de la app.
- Las apps sin suscripción pueden ofrecer un periodo de prueba gratuito por un tiempo limitado antes de presentar la opción de activación total mediante la configuración de un artículo no consumible de compra dentro de la app (IAP) a un precio 0 cuyo nombre siga la convención “prueba de XX días”. Antes del inicio de la prueba, la app debe identificar claramente su duración, el contenido o los servicios a los que ya no se podrá acceder cuando termine la prueba y cualquier costo adicional que el usuario deba pagar para disfrutar de todas las funcionalidades. Obtén más información sobre la administración del acceso al contenido y la vigencia del periodo de prueba en [Recibos](#) y [DeviceCheck](#).
- Las apps pueden usar la funcionalidad de compra dentro de la app para comercializar y vender servicios relacionados con tokens no fungibles (NFT), como la acuñación, el listado y la transferencia. Las apps pueden permitir a los usuarios ver sus propios NFT, siempre que la propiedad de los NFT no active funcionalidades dentro de la app. Se puede permitir a los usuarios explorar las colecciones de NFT de otras personas, siempre que las apps (excepto las que están en la tienda de Estados Unidos) no incluyan botones, enlaces externos ni otras llamadas a la acción

que dirijan a los clientes a otros mecanismos de compra distintos de los de las compras dentro de la app.

3.1.1(a) Enlace a otros métodos de compra

Los desarrolladores pueden solicitar derechos para proporcionar un enlace en su app a un sitio web que poseen o del que son responsables para comprar contenido o servicios digitales. Los desarrolladores no necesitan estos derechos para incluir botones, enlaces externos u otras llamadas a la acción en sus apps en la tienda de Estados Unidos. Consulta los detalles adicionales que figuran a continuación.

- **Derechos de enlace de compra externa de StoreKit:** Las apps del App Store de regiones específicas pueden ofrecer compras dentro de la app y también usar un derecho de enlace de compra externa de StoreKit para incluir un enlace al sitio web del desarrollador en el que se informe a los usuarios sobre otras formas de comprar bienes o servicios digitales. Obtén más información acerca de estos [derechos](#). Conforme a los acuerdos de derechos, el enlace puede informar a los usuarios sobre dónde y cómo comprar esos artículos de compra dentro de la app, y sobre el hecho de que dichos artículos pueden estar disponibles a un precio comparativamente más bajo. Los derechos se limitan al uso exclusivo en el App Store de iOS o iPadOS en tiendas específicas. En todas las demás tiendas, excepto la de los Estados Unidos, donde esta prohibición no se aplica, las apps y sus metadatos no pueden incluir botones, enlaces externos ni otras llamadas a la acción que dirijan a los clientes a mecanismos de compra distintos de los de las compras dentro de la app.
- **Derechos de servicios de música en streaming:** Las apps de música en streaming de determinadas regiones pueden usar los derechos de servicios de música en streaming para incluir un enlace (que puede ser un botón de compra) al sitio web del desarrollador en el que se informe a los usuarios sobre otras formas de comprar contenido o servicios de música digitales. Estos derechos también permiten a los desarrolladores de apps de música en streaming solicitar a los usuarios que proporcionen su dirección de correo electrónico con el fin expreso de enviarles un enlace al sitio web del desarrollador para comprar contenido o servicios de música digitales. Obtén más información acerca de estos [derechos](#). Conforme a los acuerdos de derechos, el enlace puede informar a los usuarios sobre dónde y cómo comprar esos artículos de compra dentro de la app, y sobre el precio de dichos artículos. Los derechos se limitan al uso exclusivo en el App Store de iOS o iPadOS en tiendas específicas. En todas las demás tiendas, las apps de música en streaming y sus metadatos no pueden incluir botones, enlaces externos u otras llamadas a la acción que dirijan a los clientes a mecanismos de compra distintos de los de las compras dentro de la app.
- Si tu app se involucra en prácticas de marketing engañosas, estafas o fraudes en relación con el derecho, se eliminará del App Store y es posible que se te expulse de Apple Developer Program.

3.1.2 Suscripciones

Las apps pueden ofrecer suscripciones de compras dentro de la app que se renueven de forma automática, independientemente de la categoría en el App Store. Cuando incorpores suscripciones de renovación automática en tu app, asegúrate de seguir los lineamientos que se indican a continuación.

3.1.2(a) Usos permitidos

Si ofreces una suscripción de renovación automática, debes proporcionar valor continuo al cliente, y el periodo de suscripción debe durar al menos siete días y estar disponible en todos los dispositivos del usuario. Si bien la siguiente lista no es exhaustiva, incluye algunos ejemplos de suscripciones adecuadas: nuevos niveles de juegos, contenido por episodios, compatibilidad con varios jugadores, apps que ofrecen frecuentemente actualizaciones importantes, acceso a contenido multimedia que se actualiza continuamente o a grandes colecciones de ese tipo de contenido, software como servicio (SAAS) y compatibilidad con la nube. Asimismo:

- Las suscripciones se pueden ofrecer junto con las ofertas a la carta (p. ej., puedes ofrecer una suscripción a una biblioteca completa de películas, así como la compra o el alquiler de una sola película).
- Los juegos que se ofrecen en una suscripción a un servicio de juego de streaming pueden ofrecer una única suscripción que se comparta en diferentes apps y servicios de terceros. Sin embargo, deben descargarse directamente del App Store, deben diseñarse para evitar el pago duplicado por parte del suscriptor y no deben poner en desventaja a los clientes no suscritos.
- Las suscripciones deben funcionar en todos los dispositivos del usuario donde la app esté disponible. Obtén más información sobre [cómo se comparte una suscripción entre diferentes apps](#).
- Al igual que con todas las apps, las que ofrecen suscripciones deben permitir que un usuario obtenga lo que pagó sin necesidad de otras actividades adicionales, como publicar en redes sociales, cargar contactos, registrarse en la app una cierta cantidad de veces, etc.
- Las suscripciones pueden incluir créditos consumibles, gemas, monedas de juegos, etc., y puedes ofrecer suscripciones que incluyen acceso a artículos consumibles con descuento (p. ej., una membresía platino que incluye paquetes de gemas por un precio reducido).
- Si tienes pensado cambiar tu app actual por un modelo de negocio basado en suscripciones, debes asegurarte de conservar la funcionalidad principal existente que los usuarios ya pagaron. Por ejemplo, procura que los clientes que ya compraron una “activación total del juego” no pierdan acceso al juego completo después de presentar el modelo de suscripción para los nuevos clientes.
- Las apps con suscripción de renovación automática pueden ofrecer un periodo de prueba gratuito a los clientes mediante la provisión de la información relevante establecida en App Store Connect. [Obtén más información sobre cómo ofrecer ofertas de suscripción](#).
- Las apps que intentan estafar a los usuarios se eliminarán del App Store. Entre estas, se incluyen las apps que intentan engañar a los usuarios para que compren una suscripción de forma fraudulenta o se involucren en prácticas de engaño y estafa. Se eliminarán del App Store, y es posible que te expulsen del Apple Developer Program.
- En las apps de operadores de telefonía móvil, se pueden incluir suscripciones a servicios de reproducción de música y video de renovación automática cuando se compren en paquetes con nuevos planes de datos móviles, previa aprobación de Apple. Es posible que también se incluyan otras suscripciones de renovación automática en los paquetes cuando se compren con nuevos planes de datos móviles, con la aprobación previa de Apple, si las apps del operador de telefonía móvil permiten a los usuarios las

compras dentro de la app. Dichas suscripciones no pueden incluir acceso a artículos consumibles ni descuentos en ellos, y su finalización debe coincidir con la finalización del plan de datos móviles.

3.1.2(b) Actualizaciones y paso a versiones anteriores

Los usuarios deben poder actualizar la suscripción y pasar a versiones anteriores sin problemas, y deben evitar suscribirse sin querer a múltiples variaciones de lo mismo. Consulta las [prácticas recomendadas](#) sobre cómo administrar las opciones para actualizar la suscripción y pasar a versiones anteriores.

3.1.2(c) Información de suscripción

Antes de pedirle a un cliente que se suscriba, debes describir claramente lo que obtendrá el usuario por el precio. ¿Cuántos lanzamientos al mes? ¿Cuánto almacenamiento en la nube? ¿Qué tipo de acceso a tu servicio? Asegúrate de comunicar claramente los requisitos descritos en [la cláusula 2 del Acuerdo de licencia de Apple Developer Program](#).

3.1.3 Otros métodos de compra

Las siguientes apps pueden usar métodos de compra distintos de las compras dentro de la app. Las apps de esta sección no pueden, dentro de la app, incentivar a los usuarios a usar un método de compra distinto de las compras dentro de la app, excepto las apps de la tienda de Estados Unidos y como se establece en 3.1.1(a) y 3.1.3(a). Los desarrolladores pueden enviar comunicaciones fuera de la app a su base de usuarios sobre métodos de compra distintos de las compras dentro de la app.

3.1.3(a) Apps de lectura

Las apps pueden permitir que un usuario acceda a contenido comprado previamente o a suscripciones de contenido (en particular, revistas, periódicos, libros, audio, música y videos). Las apps de lectura pueden ofrecer la creación de cuentas para niveles gratuitos y la funcionalidad de administración de cuentas para los clientes existentes. Los desarrolladores de apps de lectura pueden solicitar el derecho a cuenta con enlace externo para proporcionar en su app un enlace informativo a un sitio web del cual el desarrollador sea propietario o responsable para crear o administrar una cuenta. Este derecho no es necesario para que los desarrolladores incluyan botones, enlaces externos u otras llamadas a la acción en sus apps en la tienda de Estados Unidos. Obtén más información sobre el [derecho a cuenta con enlace externo](#).

3.1.3(b) Servicios multiplataforma

Las apps que funcionan en varias plataformas pueden permitir a los usuarios acceder a contenido, suscripciones o funcionalidades que hayan adquirido en tu app en otras plataformas o en tu sitio web, incluidos los artículos consumibles en juegos multiplataforma, siempre que dichos artículos también estén disponibles como [compras dentro de la app](#).

3.1.3(c) Servicios empresariales

Si solo vendes tu app directamente a organizaciones o grupos para su personal o estudiantes (p. ej., bases de datos profesionales y herramientas de administración de clases), puedes permitir que los usuarios empresariales accedan a contenido o suscripciones que hayan adquirido antes. Para las ventas al consumidor, a un único usuario o a una familia, se debe usar la funcionalidad de compra dentro de la app.

3.1.3(d) Servicios de persona a persona

Si tu app permite la compra de servicios de persona a persona en tiempo real entre dos personas (p. ej., clases particulares a estudiantes, consultas médicas, visitas inmobiliarias o entrenamiento físico), puedes usar métodos de compra distintos de las compras dentro de la app para cobrar esos pagos. Para los servicios en tiempo real entre una y pocas personas o entre una y varias personas, se debe usar la funcionalidad de compra dentro de la app.

3.1.3(e) Productos y servicios fuera de la app

Si tu app permite que las personas compren bienes o servicios físicos que se consumirán fuera de la app, debes usar métodos de compra distintos de la compra dentro de la app para cobrar esos pagos, como Apple Pay o el método con tarjeta de crédito tradicional.

3.1.3(f) Apps independientes y gratuitas

Las apps gratuitas que actúan como complemento independiente de una herramienta web de pago (p. ej., VoIP, almacenamiento en la nube, servicios de correo electrónico, alojamiento web) no necesitan usar la funcionalidad de compra dentro de la app, siempre que no se realicen compras dentro de la app ni llamadas a la acción para realizar compras fuera de la app.

3.1.3(g) Apps de administración de publicidad

No es necesario que las apps que tienen como único propósito permitir a los anunciantes (personas o empresas que publicitan un producto, servicio o evento) comprar y administrar campañas publicitarias en distintos tipos de medios (televisión, exteriores, sitios web, apps, etc.) hagan uso de la funcionalidad de compra dentro de la app. Estas apps están diseñadas para fines de administración de campañas y no muestran los anuncios. Las compras digitales de contenido que se experimenta o se consume en una app, incluida la compra de anuncios para mostrar en la misma app (como la venta de "mejoras" para publicaciones en una app de redes sociales), se deben realizar mediante la funcionalidad de compra dentro de la app.

3.1.4 Contenido específico del hardware

En circunstancias limitadas, como cuando las funcionalidades dependen de un hardware específico para su uso, la app puede activar esa funcionalidad sin la necesidad de usar la funcionalidad de compra dentro de la app (p. ej., una app de astronomía que agrega funcionalidades cuando se sincroniza con un telescopio). Las funcionalidades de la app que se usan junto con un producto físico aprobado (como un juguete) de forma opcional pueden activar la funcionalidad sin la necesidad de usar la funcionalidad de compra dentro de la app, siempre que también haya disponible una opción de compra dentro de la app.

Sin embargo, no puedes exigir a los usuarios que compren productos que no estén relacionados ni que interactúen con campañas publicitarias o de marketing para activar la funcionalidad de la app.

3.1.5 Criptomonedas

- (i) Carteras:** Las apps pueden facilitar el almacenamiento de monedas virtuales, siempre que las ofrezcan desarrolladores inscritos como organización.
- (ii) Minería:** Las apps no pueden minar criptomonedas a menos que el procesamiento se realice fuera del dispositivo (p. ej., minería basada en la nube).
- (iii) Intercambios:** Las apps pueden facilitar la transacción o la transmisión de criptomonedas mediante un intercambio aprobado, siempre que se ofrezcan solo en países o regiones en los que la app cuente con las licencias y los permisos adecuados para ofrecer el servicio de intercambio de criptomonedas.
- (iv) Ofertas iniciales de monedas:** Las apps que facilitan las ofertas iniciales de monedas (ICO), la comercialización de futuros de criptomonedas y otras operaciones de criptovalores o cuasivalores deben proceder de bancos establecidos, empresas de valores, comerciantes de comisiones de futuros (FCM), u otras instituciones financieras autorizadas y deben cumplir con todas las leyes aplicables.
- (v) Las apps de criptomonedas no pueden ofrecer divisas por completar tareas, tales como** descargar otras apps, instar a otros usuarios a descargarlas, publicar en redes sociales, etc.

3.2 Otros asuntos relativos al modelo de negocio

Las listas que aparecen a continuación no son exhaustivas y es posible que tu envío genere un cambio o una actualización de nuestras políticas, pero hay algunas otras recomendaciones y prohibiciones que debes tener en cuenta:

3.2.1 Prácticas aceptables

- (i) Mostrar tus propias apps para venderlas o promocionarlas dentro de la app, siempre que esta no sea solo un catálogo de apps.**
- (ii) Mostrar o recomendar una colección de apps de terceros diseñadas para una necesidad específica aprobada (p. ej., administración de la salud, aviación, accesibilidad). Tu app debe proporcionar un contenido editorial sólido para que no parezca una simple tienda.**
- (iii) Deshabilitar el acceso a determinado contenido aprobado para alquilar (p. ej., películas, programas de televisión, música, libros) después de que expire el periodo de alquiler. El resto de los artículos y servicios no pueden vencer.**

(iv) Los pases de Wallet se pueden usar para efectuar o recibir pagos, transmitir ofertas u ofrecer identificación (como entradas para el cine, cupones y credenciales VIP). Otros usos pueden provocar el rechazo de la app y la revocación de las credenciales de Wallet.

(v) Las apps de seguros deben ser gratuitas, cumplir con las leyes de las regiones donde se distribuyen y no pueden usar la funcionalidad de compra dentro de la app.

(vi) Las organizaciones sin fines de lucro autorizadas pueden recaudar fondos directamente dentro de sus propias apps o apps de terceros, siempre que esas campañas de recaudación de fondos cumplan con todos los lineamientos de revisión de apps y sean compatibles con Apple Pay. Estas apps deben indicar cómo se usarán los fondos, cumplir con todas las leyes locales y federales requeridas, y garantizar que los recibos de impuestos correspondientes estén disponibles para los donantes. Se debe proporcionar información adicional al equipo de App Review si este la solicita. Las plataformas de organizaciones sin fines de lucro que conectan a los donantes con otras organizaciones sin fines de lucro deben garantizar que todas las organizaciones incluidas en la app también hayan pasado por el proceso de autorización pertinente. Obtén más información sobre cómo convertirte en una [organización sin fines de lucro autorizada](#).

(vii) Las apps pueden permitir a los usuarios ofrecer un donativo monetario a otra persona sin usar la funcionalidad de compra dentro de la app, siempre que (a) el donativo sea una opción completamente opcional del donante y (b) el 100% de los fondos se destinen al receptor del donativo. Sin embargo, los donativos que estén relacionados o asociados en algún momento con la recepción de contenido o servicios digitales deben usar la funcionalidad de compra dentro de la app.

(viii) Las apps que se usan para transacciones financieras, inversiones o administración de dinero se deben enviar mediante la institución financiera que presta dichos servicios y deben tener las licencias y los permisos necesarios en las ubicaciones donde se ofrezcan.

3.2.2 Prácticas inaceptables

(i) Crear una interfaz para mostrar apps, extensiones o plug-ins de terceros similares al App Store o como una colección de interés general.

(ii) Se omitió intencionalmente.

(iii) Usar medios artificiales para aumentar la cantidad de impresiones o clics de los anuncios, así como las apps que están diseñadas principalmente para mostrar anuncios.

(iv) A menos que seas una de las organizaciones sin fines de lucro aprobadas o permitidas según la sección 3.2.1 (vi) mencionada anteriormente, recaudar dinero dentro de la app para entidades benéficas o recaudadoras de fondos. Las apps que tengan como fin recaudar dinero para tales causas deben ser gratuitas en el App Store y solo pueden recaudar fondos fuera de la app, por ejemplo, a través de Safari o SMS.

(v) Restringir arbitrariamente quién puede usar la app, por ejemplo, según la ubicación o el operador.

(vi) Se omitió intencionalmente.

(vii) Manipular artificialmente la visibilidad, el estado o la clasificación de un usuario en otros servicios, a menos que esté permitido por los Términos y condiciones de ese servicio.

(viii) Las apps que facilitan la comercialización de opciones binarias no están permitidas en el App Store. Como alternativa, analiza la posibilidad de usar una app web. Las apps que facilitan la comercialización de contratos por diferencias (CFD) u otros derivados (p. ej., FOREX) deben tener la licencia correspondiente en todas las jurisdicciones donde el servicio está disponible.

(ix) Las apps que ofrecen préstamos personales deben indicar de forma clara y visible todos los términos del préstamo, incluidos, entre otros, la tasa de porcentaje anual (APR) máxima equivalente y la fecha de vencimiento del pago. Las apps de préstamos no pueden cobrar una APR máxima superior al 36%, incluidos los costos y las tarifas, y no pueden exigir la devolución del préstamo en 60 días o menos.

(x) Las apps no deben obligar a los usuarios a brindar calificaciones, escribir reseñas, descargar otras apps ni realizar ninguna otra acción similar para poder acceder a sus funcionalidades, contenido o uso. En su lugar, las apps pueden motivar a los usuarios a realizar acciones específicas dentro de las apps (por ejemplo, completar un nivel o ver un anuncio).

4. Diseño

Los clientes de Apple valoran mucho los productos que son simples, refinados, innovadores y fáciles de usar, y eso es lo que queremos ver en el App Store. La creación de un gran diseño depende de ti, pero las siguientes son las normas mínimas para su aprobación en el App Store. Recuerda que, incluso después de que tu app se apruebe, debes actualizarla para asegurarte de que conserve su funcionalidad y siga siendo atractiva para los clientes nuevos y existentes. Las apps que dejan de funcionar o que ofrecen una experiencia deficiente pueden eliminarse del App Store en cualquier momento.

4.1 Imitaciones

(a) Aporta tus propias ideas. Sabemos que las tienes. Solo tienes que hacerlas realidad. No te limites a copiar la app más reciente del App Store ni a hacer cambios mínimos en el nombre o la interfaz de usuario de otra app y finjas que es tuya. Además de arriesgarte a una demanda por infracción de la propiedad intelectual, dificultarás la navegación por el App Store y será injusto para tus colegas desarrolladores.

(b) ➡ Enviar apps que se hacen pasar por otras apps o servicios se considera una infracción del Código de conducta para desarrolladores y puede dar lugar a la eliminación de Apple Developer Program.

(c) No puedes usar el ícono, la marca ni el nombre del producto de otro desarrollador en el ícono o el nombre de tu app sin la aprobación del desarrollador.

4.2 Funcionalidad mínima

Tu app debe incluir funcionalidades, contenido y una interfaz de usuario que le permitan ser más que un simple sitio web renovado. Si tu app no es realmente útil o única, o si no tiene el aspecto típico de una app, no debe estar en el App Store. Si tu app no ofrece algún tipo de entretenimiento duradero o utilidad adecuada, puede que no se acepte. Las apps que solo sean una canción o una película deben enviarse al iTunes Store. Las apps que solo sean un libro o un juego deben enviarse al Apple Books Store.

4.2.1 Las apps que usan ARKit deben brindar experiencias de realidad aumentada completas e integradas. No basta con colocar un modelo en una vista de realidad aumentada o reproducir una animación.

4.2.2 A menos que sean catálogos, las apps no deben ser principalmente materiales de marketing, anuncios, recortes web, recopiladores de contenido o una colección de enlaces.

4.2.3

(i) La app debería funcionar por sí sola sin necesidad de instalar otra app.

(ii) Si tu app necesita descargar otros recursos para funcionar al abrirse por primera vez, indica el tamaño de la descarga y avisa a los usuarios antes de que inicien la descarga.

4.2.4 Se omitió intencionalmente.

4.2.5 Se omitió intencionalmente.

4.2.6 Las apps creadas a partir de una plantilla comercializada o un servicio de generación de apps se rechazarán, a menos que el proveedor del contenido de la app las envíe directamente. Estos servicios no deben enviar apps en nombre de sus clientes y deben ofrecer herramientas que les permitan crear apps personalizadas e innovadoras que brinden experiencias únicas a los usuarios. Otra opción aceptable para los proveedores de plantillas es crear un archivo binario único donde se aloje todo el contenido del cliente en un modelo de agregación o "selector", por ejemplo, una app de búsqueda de restaurantes con diferentes entradas o páginas personalizadas para cada restaurante del cliente, o una app de eventos con diferentes entradas para cada evento del cliente.

4.2.7 Clientes de escritorio remoto

Si tu app de escritorio remoto funciona como un reflejo exacto de un software o servicio específico, no como un reflejo genérico del dispositivo principal, debe cumplir los siguientes requisitos:

(a) La app solo debe conectarse a un dispositivo principal del usuario que sea una computadora personal o una consola de juegos del usuario, y tanto el dispositivo principal como el cliente deben estar conectados a una red LAN local.

(b) El software o los servicios que aparezcan en el cliente deben ejecutarse por completo en el dispositivo principal, deben reflejarse en la pantalla del dispositivo principal y no deben usar las API ni

las funcionalidades de la plataforma para otros fines que no sean la reproducción en streaming del escritorio remoto.

(c) Toda la creación y administración de cuentas debe iniciarse desde el dispositivo principal.

(d) La interfaz de usuario que aparece en el cliente no debe parecerse a una vista de iOS o del App Store, no debe tener la apariencia de una tienda ni incluir la posibilidad de explorar, seleccionar o comprar software cuya titularidad o licencia no sea ya del usuario. Para mayor claridad, no es necesario que las transacciones que se realizan dentro del software duplicado usen la funcionalidad de compra dentro de la app, siempre que las transacciones se procesen en el dispositivo principal.

(e) Los clientes ligeros de apps basadas en la nube no son adecuados para el App Store.

4.3 Spam

(a) ➡ No crees varios ID de paquete de la misma app. Si tu app tiene diferentes versiones para determinados lugares, equipos deportivos, universidades, etc., considera enviar una sola app y ofrecer las variantes mediante compras dentro de la app.

(b) Evita también sobrecargar una categoría saturada. En el App Store ya hay suficientes apps de ruido de flatulencias o eructos, de linternas, de predicción del futuro, de citas, de juegos para beber, de Kamasutra, etc. Rechazaremos estas apps a menos que brinden una experiencia única y de alta calidad. Colmar la tienda de contenido no deseado puede dar como resultado la expulsión de Apple Developer Program.

4.4 ➡ Extensiones

Las apps que alojen o contengan extensiones deben cumplir con la [Guía de programación de extensiones de apps](#), la [documentación de extensiones de apps de Safari](#) o la [documentación de extensiones web de Safari](#), y deben incluir la misma funcionalidad, como pantallas de ayuda e interfaces de configuración si es posible. Debes indicar de forma clara y precisa en el texto de marketing de la app qué extensiones están disponibles, y estas no pueden incluir anuncios, publicidad ni compras dentro de la app.

4.4.1 ➡ Las extensiones de teclado tienen algunas reglas adicionales.

Qué deben hacer:

- Proporcionar la funcionalidad de entrada de datos mediante el teclado (p. ej., caracteres escritos).
- Seguir los lineamientos de los stickers si el teclado incluye imágenes o emojis.
- Proporcionar un método para avanzar al siguiente teclado.
- Seguir funcionando sin acceso total a la red y sin requerir acceso completo.
- Recopilar la actividad del usuario solo para mejorar la funcionalidad de la extensión del teclado del usuario en el dispositivo iOS.

Qué no deben hacer:

- Abrir otras apps además de Configuración.
- Cambiar la función de los botones del teclado para que tengan otros comportamientos (por ejemplo, mantener presionada la tecla de retorno para abrir la cámara).

4.4.2 ➡ Las extensiones de Safari deben ejecutarse en la versión actual de Safari en el sistema operativo de Apple correspondiente. No deben interferir con los elementos de la interfaz de usuario del sistema ni de Safari y tampoco deben incluir contenido o código malicioso o engañoso. La infracción de esta regla provocará la eliminación de Apple Developer Program. Las extensiones de Safari no deben exigir el acceso a más sitios web de los que sean estrictamente necesarios para funcionar.

4.4.3 Se omitió intencionalmente.

4.5 ➡ **Sitios y servicios de Apple**

4.5.1 ➡ Las apps pueden usar feeds RSS aprobados de Apple, como el feed RSS de iTunes Store, pero no pueden extraer ningún tipo de información de los sitios de Apple (p. ej., apple.com/la, iTunes Store, App Store, App Store Connect, portal para desarrolladores, etc.) o crear clasificaciones con esta información.

4.5.2 ➡ **Apple Music**

(i) MusicKit en iOS permite a los usuarios reproducir Apple Music y su biblioteca de música local de forma nativa desde tus apps y juegos. Cuando un usuario otorga permiso a su cuenta de Apple Music, tu app puede crear listas de reproducción, agregar canciones a su biblioteca y reproducir cualquiera de los millones de canciones del catálogo de Apple Music. Los usuarios deben iniciar la reproducción en streaming del contenido de Apple Music y poder navegar con los controles multimedia estándar, como “reproducir”, “pausar” y “omitir”. Además, tu app no debe solicitar pagos ni monetizar indirectamente el acceso al servicio de Apple Music (p. ej., compras dentro de la app, publicidad, solicitud de información del usuario, etc.). No descargues, cargues ni actives el uso compartido de archivos de música provenientes de las API de MusicKit, excepto en los casos explícitamente permitidos en la documentación de [MusicKit](#).

(ii) El uso de las API de MusicKit no reemplaza la protección de las licencias que podrías necesitar para una integración musical más profunda o compleja. Por ejemplo, si quieres que tu app reproduzca una canción específica en un momento particular, o que cree archivos de audio o video que se puedan compartir en las redes sociales, deberás comunicarte directamente con los titulares de los derechos para obtener su permiso (p. ej., derechos de sincronización o adaptación) y materiales. La imagen de portada y otros metadatos solo pueden usarse en relación con la reproducción de música o las listas de reproducción (incluidas las capturas de pantalla en las que se muestra la funcionalidad de la app) y no deben usarse en ningún anuncio o publicidad sin la autorización específica de los titulares de los derechos. Asegúrate de seguir los [Lineamientos de identidad de Apple Music](#) al integrar los servicios de Apple Music en tu app.

(iii) Las apps que acceden a los datos de los usuarios de Apple Music, como las listas de reproducción y los favoritos, deben indicar claramente este acceso en el texto donde se describe su propósito. Los datos recopilados no se pueden compartir con terceros para ningún otro propósito que

no sea respaldar o mejorar la experiencia de la app. Estos datos no se pueden usar para identificar usuarios o dispositivos, ni para dirigir las publicidades.

4.5.3 ➡ No uses los servicios de Apple, como Game Center, notificaciones push, etc., para enviar mensajes de spam, de suplantación de identidad (phishing) o no deseados a los clientes. No intentes hacer búsquedas inversas, rastrear, relacionar, asociar, minar, recopilar ni explotar de ningún otro modo los ID de los jugadores, sus alias ni otros datos obtenidos a través de Game Center, o se te expulsará de Apple Developer Program.

4.5.4 ➡ Las notificaciones push no deben ser necesarias para que la app funcione y no deben usarse para enviar información personal o confidencial. Las notificaciones push no se deben usar para fines promocionales ni de marketing directo, a menos que los clientes hayan optado explícitamente por recibirlos mediante un consentimiento escrito que se visualice en la interfaz de usuario de tu app y que tú proporciones un método en la app para que los usuarios cancelen la recepción de estos mensajes. El uso indebido de estos servicios puede dar como resultado la revocación de tus privilegios.

4.5.5 ➡ Solo usa los ID de jugador de Game Center de la manera aprobada por los términos de Game Center y no los muestres en la app ni a terceros.

4.5.6 ➡ Las apps pueden usar caracteres Unicode que se vean como emojis de Apple en la app y en los metadatos. Los emojis de Apple no pueden usarse en otras plataformas ni integrarse directamente en el archivo binario de la app.

4.6 Se omitió intencionalmente.

4.7 ➡ Miniapps, minijuegos, juegos de streaming, chatbots, plug-ins y emuladores de juegos

Las apps pueden ofrecer ciertos tipos de software que no están integrados en el archivo binario, específicamente miniapps y minijuegos HTML5 y JavaScript, juegos de streaming, chatbots y plug-ins. Además, las apps de emulador de videoconsolas y PC retro ofrecen la posibilidad de descargar juegos. Eres responsable de todos los tipos de software que se ofrecen en tu app, lo que incluye garantizar que el software cumpla con estos lineamientos y todas las leyes aplicables. El software que no cumpla con uno o más lineamientos será motivo de rechazo de tu app. También debes asegurarte de que el software cumpla con las reglas adicionales que se indican en los lineamientos de la sección 4.7.1 a la sección 4.7.5. Estas reglas adicionales son importantes para preservar la experiencia que esperan los clientes del App Store y para garantizar la seguridad de los usuarios.

4.7.1 El software que se ofrece en las apps según esta regla debe:

- seguir todos los lineamientos de privacidad, incluidas, entre otras, las reglas establecidas en el lineamiento 5.1 relativas a la recopilación, el uso y el intercambio de información y datos confidenciales (como datos de salud y datos personales de menores de edad);
- incluir un método para filtrar el material censurable, un mecanismo para denunciar el contenido y brindar respuestas oportunas a las inquietudes y la capacidad de bloquear a los usuarios que hacen uso indebido; y

- seguir el lineamiento 3.1 para ofrecer bienes o servicios digitales a los usuarios finales.

4.7.2 🚫 Tu app no puede extender ni exponer las tecnologías o API nativas de la plataforma al software sin el permiso previo de Apple.

4.7.3 🚫 Tu app no puede compartir datos ni permisos de privacidad con ningún software individual que se ofrece en ella sin el consentimiento explícito del usuario en cada caso.

4.7.4 Debes proporcionar un índice de software y metadatos disponibles en tu app. Este debe incluir enlaces universales a todos los tipos de software que se ofrecen en tu app.

4.7.5 🚫 Tu app debe proporcionar una manera para que los usuarios identifiquen el software que supera la clasificación por edad de la app y usar un mecanismo de restricción de edad basado en la edad verificada o declarada para limitar el acceso de los usuarios menores de edad.

4.8 🚫 **Servicios de inicio de sesión**

Las apps que usen el servicio de inicio de sesión de una red social o de terceros (como inicio de sesión con Facebook, inicio de sesión con Google, inicio de sesión con Twitter, inicio de sesión con LinkedIn, inicio de sesión con Amazon o inicio de sesión de WeChat) para configurar o autenticar la cuenta principal del usuario con la app también deben ofrecer como opción equivalente otro servicio de inicio de sesión con las siguientes funcionalidades:

- el servicio de inicio de sesión debe limitar la recopilación de datos al nombre y la dirección de correo electrónico del usuario;
- el servicio de inicio de sesión debe permitir a los usuarios mantener su dirección de correo electrónico privada como parte de la configuración de su cuenta; y
- el servicio de inicio de sesión no debe recopilar interacciones con tu app para fines publicitarios sin consentimiento.

La cuenta principal de un usuario es la que este establece con tu app con el fin de identificarse, iniciar sesión y acceder a las funcionalidades y los servicios asociados.

No se requiere otro servicio de inicio de sesión si:

- Tu app usa exclusivamente los sistemas de inicio de sesión y la configuración de la cuenta de tu empresa.
- Tu app es un mercado de apps alternativo, o una app distribuida desde un mercado de apps alternativo, que usa un inicio de sesión específico del mercado para funcionalidades de cuenta, descarga y comercio.
- Tu app es una app educativa, empresarial o de negocios que requiere que el usuario inicie sesión con una cuenta educativa o empresarial existente.

- Tu app usa un sistema de identificación de ciudadanos o un sistema de identificación electrónica respaldado por el gobierno o la industria para autenticar a los usuarios.
- Tu app es cliente de un servicio externo específico y los usuarios deben iniciar sesión en su correo, redes sociales u otra cuenta de terceros directamente para acceder a su contenido.

4.9 Apple Pay

Las apps que usan Apple Pay deben proporcionar al usuario toda la información relativa a la compra antes de proceder con la venta de cualquier bien o servicio, y deben usar correctamente los elementos de la interfaz de usuario y la marca de Apple Pay, tal como se describe en los Lineamientos de marketing de Apple Pay y en las Human Interface Guidelines. Las apps que usan Apple Pay para ofrecer pagos recurrentes deben, como mínimo, revelar la siguiente información:

- La duración del plazo de renovación y el hecho de que continuará en vigor hasta la cancelación.
- Qué se proporcionará durante cada periodo.
- Los cargos reales que se facturarán al cliente.
- Cómo realizar la cancelación.

4.10 Monetización de las capacidades integradas

No puedes monetizar las capacidades integradas proporcionadas por el hardware o el sistema operativo, como las notificaciones push, la cámara o el giroscopio, ni los servicios y las tecnologías de Apple, como el acceso a Apple Music, el almacenamiento de iCloud o las API de Tiempo en pantalla.

5. Legal

Las apps deben cumplir con todos los requisitos legales de todos los lugares donde estén disponibles (si tienes dudas al respecto, consulta con un abogado). Sabemos que esto es complicado, pero es tu responsabilidad comprender y asegurarte de que tu app cumpla con todas las leyes locales, no solo con los lineamientos que se indican a continuación. Además, por supuesto, se rechazarán las apps que soliciten, promuevan o fomenten un comportamiento delictivo o claramente imprudente. En casos extremos, como las apps que facilitan la trata de personas o la explotación de niños, se notificará a las autoridades correspondientes.

5.1 🚫 Privacidad

La protección de la privacidad del usuario es fundamental en el ecosistema de Apple, y debes tener cuidado al usar datos personales para asegurarte de cumplir las [prácticas recomendadas de privacidad](#), las leyes aplicables y los términos del [Acuerdo de licencia de Apple Developer Program](#), además de las expectativas de los clientes. Más específicamente:

5.1.1 🚫 Recopilación y almacenamiento de datos

(i) Políticas de privacidad: Todas las apps deben incluir un enlace a su política de privacidad en el campo de metadatos de App Store Connect y dentro de la app de una manera fácilmente accesible. La política de privacidad debe ser clara y explícita con lo siguiente:

- Identificar qué datos, si los hay, recopila la app o el servicio, cómo recopila esos datos y todos los usos de esos datos.
- Confirmar que cualquier tercero con quien la app comparta los datos del usuario (de acuerdo con estos lineamientos), como herramientas de análisis, redes de publicidad y SDK de terceros, así como cualquier entidad principal, subsidiaria u otra entidad relacionada que tenga acceso a dichos datos, ofrecerá un nivel de protección de los datos del usuario igual o equivalente al establecido en la política de privacidad de la app y en estos lineamientos.
- Explicar sus políticas de retención o eliminación de datos y describir cómo los usuarios pueden revocar el consentimiento o solicitar la eliminación de sus datos.

(ii) Permiso: Las apps que recopilan datos del usuario o del uso deben obtener el consentimiento del usuario para la recopilación, incluso si dichos datos se consideran anónimos en el momento de la recopilación o inmediatamente después. La funcionalidad de pago no debe exigir que un usuario otorgue acceso a estos datos ni debe depender de eso. Las apps también deben proporcionar al cliente una forma fácilmente accesible y comprensible de retirar su consentimiento. Asegúrate de que en el texto del propósito se describa de forma clara y completa el uso que se hará de los datos. Las apps que recopilan datos para un interés legítimo sin consentimiento de conformidad con los términos del Reglamento General de Protección de Datos (GDPR) de la Unión Europea o estatutos similares deben cumplir con todos los términos de esa ley. Obtén más información sobre [cómo solicitar permiso](#).

(iii) Minimización de datos: Las apps solo deben solicitar acceso a los datos relevantes para su funcionalidad principal y solo deben recopilar y usar los datos necesarios para cumplir con la tarea que corresponda. Siempre que sea posible, usa el selector fuera del proceso o un menú Compartir en lugar de solicitar el acceso total a recursos protegidos, como Fotos o Contactos.

(iv) Acceso: Las apps deben respetar la configuración de permisos del usuario y no intentar manipular, engañar ni forzar a las personas a dar su consentimiento para el acceso a datos innecesarios. Por ejemplo, las apps que incluyen la posibilidad de publicar fotos en una red social tampoco deben requerir acceso al micrófono antes de permitir al usuario cargar las fotos. Siempre que sea posible, brinda soluciones alternativas para los usuarios que no otorgan su consentimiento.

Por ejemplo, si un usuario se niega a compartir la ubicación, ofrece la posibilidad de ingresar manualmente una dirección.

(v) Inicio de sesión en la cuenta: Si tu app no incluye funcionalidades importantes basadas en cuentas, permite que las personas la usen sin iniciar sesión. Si tu app admite la creación de cuentas, también debes [ofrecer la eliminación de la cuenta dentro de la app](#). Las apps no pueden solicitar a los usuarios el ingreso de información personal para funcionar, a menos que sea directamente relevante para la funcionalidad principal de la app o que la ley lo exija. Si la funcionalidad principal de tu app no está relacionada con una red social específica (p. ej., Facebook, WeChat, Weibo, X, etc.), debes proporcionar acceso sin inicio de sesión o mediante otro mecanismo. Obtener información básica del perfil, compartirla en redes sociales o invitar a amigos a usar la app no se consideran funcionalidades principales de la app. La app también debe incluir un mecanismo para revocar las credenciales de las redes sociales y desactivar el acceso a los datos entre la app y las redes sociales desde dentro de la app. Una app no puede almacenar fuera del dispositivo credenciales ni tokens que permitan ingresar a redes sociales y solo puede usar dichas credenciales o tokens para conectarse directamente a las redes sociales desde la propia app mientras la app está en uso.

(vi) Los desarrolladores que usen sus apps para descubrir secretamente contraseñas u otros datos privados serán expulsados de Apple Developer Program.

(vii) SafariViewController debe usarse para presentar información visible a los usuarios; el controlador no puede estar oculto ni quedar opacado por otras vistas o capas. Además, una app no puede usar SafariViewController para rastrear a los usuarios sin su conocimiento y consentimiento.

(viii) Las apps que recopilan información personal de cualquier fuente que no sea directamente del usuario o sin el consentimiento explícito del usuario, incluso bases de datos públicas, no están permitidas en el App Store ni a través de una distribución alternativa.

(ix) Las apps que brindan servicios en campos altamente regulados (como servicios bancarios y financieros, atención médica, juegos de azar, consumo legal de cannabis, viajes aéreos y plataformas de criptomonedas) o que requieren información confidencial del usuario deben ser enviadas por una entidad legal que brinde los servicios, no por un desarrollador individual. Las apps que facilitan la venta legal de cannabis deben estar restringidas geográficamente a la jurisdicción legal correspondiente.

(x) Las apps pueden solicitar información de contacto básica (como el nombre y la dirección de correo electrónico) siempre y cuando la solicitud sea opcional para el usuario, las funcionalidades y los servicios no estén condicionados a proporcionar la información y cumplan con todas las demás disposiciones de estos lineamientos, incluidas las limitaciones de recopilar información de los niños.

5.1.2 🔄 Uso e intercambio de datos

(i) A menos que la ley permita lo contrario, no puedes usar, transmitir ni compartir los datos personales de una persona sin antes obtener su permiso. Debes proporcionar acceso a la información sobre cómo y dónde se usarán los datos. Debes indicar de forma clara dónde se compartirán los datos personales con terceros, incluida la IA de terceros, y obtener un permiso explícito antes de hacerlo. Los datos recopilados de las apps solo se pueden compartir con terceros para mejorar la app

o mostrar publicidad (de acuerdo con el [Acuerdo de licencia de Apple Developer Program](#)). Debes recibir el permiso explícito de los usuarios a través de las API de transparencia del rastreo en apps para rastrear su actividad. Obtén más información sobre el [rastreo](#). Tu app no debe requerir que los usuarios activen funcionalidades del sistema (p. ej., notificaciones push, servicios de ubicación, rastreo) para acceder a la funcionalidad o el contenido, usar la app o recibir una compensación monetaria o de otro tipo, incluidos, entre otros, los códigos y las tarjetas de regalo. Las apps que comparten datos del usuario sin su consentimiento o sin cumplir con las leyes de privacidad de datos se pueden retirar del mercado y pueden dar lugar a la expulsión de Apple Developer Program.

(ii) Los datos recopilados para un propósito no se pueden volver a usar sin un consentimiento previo, a menos que la ley permita lo contrario.

(iii) Las apps no deben tratar de generar secretamente un perfil de usuario a partir de los datos recopilados y no pueden intentar, facilitar ni fomentar que otras personas identifiquen a usuarios anónimos o reconstruyan perfiles de usuarios a partir de datos recopilados de las API proporcionadas por Apple ni de ningún otro dato que indiques se haya recopilado de forma "anónima", "acumulativa" o no identificable de otro modo.

(iv) No uses información de Contactos, Fotos u otras API que accedan a datos del usuario para crear una base de datos de contactos para tu propio uso o para la venta o distribución a terceros, y no recopiles información sobre qué otras apps están instaladas en el dispositivo de un usuario con fines de análisis, publicidad o marketing.

(v) No uses la información recopilada mediante Contactos o Fotos de un usuario para comunicarte con las personas, a menos que ese usuario tenga la iniciativa explícita de hacerlo individualmente, y no incluyas una opción para seleccionar todos los contactos ni establezcas esta opción de forma predeterminada. Debes proporcionar al usuario una descripción clara del aspecto que tendrá el mensaje para el destinatario antes de enviarlo (p. ej., qué dirá el mensaje y quién aparecerá como remitente).

(vi) Los datos recopilados a partir de la API de HomeKit, HealthKit o ClassKit, la API de expedientes clínicos, las API de MovementDisorder o las herramientas de mapas de profundidad o faciales (p. ej., ARKit, API de Cámara o API de Fotos) no se pueden usar con fines publicitarios, de marketing u otros fines de extracción de datos basados en el uso, incluso por parte de terceros. Obtén más información sobre las prácticas recomendadas para la implementación de [CallKit](#), [HealthKit](#), [ClassKit](#) y [ARKit](#).

(vii) Las apps que usan Apple Pay solo pueden compartir los datos del usuario adquiridos a través de Apple Pay con terceros para facilitar o mejorar la entrega de bienes y servicios.

5.1.3 ➡ Salud e investigación médica

Los datos médicos, de salud y de bienestar son especialmente confidenciales, y las apps de este sector tienen algunas reglas adicionales para garantizar la protección de la privacidad de los clientes:

(i) Las apps no pueden usar ni divulgar a terceros datos recopilados en el contexto de la salud, el bienestar y la investigación médica, incluidos los de la API de expedientes clínicos, la API de HealthKit, la API de condición y actividad física, las API de MovementDisorder y las investigaciones con seres humanos relacionadas con la salud, con fines publicitarios, de marketing u otros fines de

extracción de datos basados en el uso que no sean la mejora de la administración de la salud o la investigación médica, y en tales casos, solo se pueden usar con autorización. Sin embargo, las apps pueden usar los datos de salud o bienestar de un usuario para proporcionar un beneficio directamente a ese usuario (como una reducción de la prima del seguro), siempre que la app sea presentada por la entidad que proporciona el beneficio y los datos no se compartan con terceros. Debes revelar los datos de salud específicos que estás recopilando del dispositivo.

(ii) Las apps no deben escribir datos falsos o inexactos en HealthKit ni en ninguna otra app de investigación médica o administración de la salud, y no pueden almacenar información médica personal en iCloud.

(iii) Las apps que realizan investigaciones con seres humanos relacionadas con la salud deben obtener el consentimiento de los participantes o, en el caso de los menores, de sus padres o tutores. Dicho consentimiento debe incluir (a) la naturaleza, el propósito y la duración de la investigación; (b) los procedimientos, los riesgos y los beneficios para el participante; (c) información sobre la confidencialidad y el uso de los datos (incluido el intercambio de datos con terceros); (d) un punto de contacto para las preguntas de los participantes; y (e) el proceso de retiro.

(iv) Las apps que realizan investigaciones con seres humanos relacionadas con la salud deben obtener la aprobación de una junta de revisión de ética independiente. Se debe proporcionar una prueba de dicha aprobación previa solicitud.

5.1.4 Niños

(a) ➡ Hay muchas razones por las cuales es importante tratar los datos personales de los niños con cuidado, y te recomendamos que leas detenidamente todos los requisitos de cumplimiento de leyes como la Ley de Protección de la Privacidad Infantil en Internet (COPPA), el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y cualquier otro reglamento o ley aplicable.

Las apps pueden solicitar la fecha de nacimiento y la información de contacto de los padres solo con el fin de cumplir con estos estatutos, pero deben incluir un valor de funcionalidad o entretenimiento útil, independientemente de la edad de la persona.

Las apps destinadas principalmente a niños no deben incluir análisis ni publicidad de terceros. Esto brinda una experiencia más segura para los niños.

(b) En muy pocos casos, se puede permitir el análisis y la publicidad de terceros, siempre que los servicios cumplan con los mismos términos estipulados en el [lineamiento 1.3](#).

Además, las apps de la categoría Niños o aquellas que recopilan, transmiten o tienen la capacidad de compartir información personal (p. ej., nombre, dirección, correo electrónico, ubicación, fotos, videos, dibujos, la capacidad de chatear, otros datos personales o identificadores persistentes que se usen en combinación con cualquiera de los anteriores) de un menor deben incluir una política de privacidad y deben cumplir con todos los estatutos de privacidad infantil pertinentes. Para no dejar lugar a dudas, el [requisito del control parental](#) de la categoría Niños no suele ser lo mismo que obtener el consentimiento parental para la recopilación de datos personales según estos estatutos de privacidad.

Recuerda que, según el [lineamiento 2.3.8](#), el uso de términos como “Para niños” y “Para menores” en los metadatos de la app se reserva para la categoría Niños. Las apps que no pertenezcan a la categoría Niños no pueden incluir ningún término en el nombre, el subtítulo, el ícono, las capturas de pantalla ni la descripción de la app que implique que los destinatarios principales de la app son niños.

5.1.5 Localización

Usa la funcionalidad Localización en tu app solo cuando sea directamente relevante para las funcionalidades y los servicios que brinda la app. Las API basadas en la ubicación no deben usarse para proporcionar servicios de emergencia o control autónomo de vehículos, aeronaves y otros dispositivos, a excepción de dispositivos pequeños, como drones y juguetes livianos, o sistemas de alarma de control remoto para automóviles, etc. Asegúrate de notificar al usuario y obtener su consentimiento antes de recopilar, transmitir o usar datos de ubicación. Si tu app usa la funcionalidad Localización, asegúrate de explicar su propósito. Consulta [Human Interface Guidelines](#) para conocer las prácticas recomendadas pertinentes.

5.2 Propiedad intelectual

Asegúrate de que tu app solo incluya contenido que creaste o que tienes licencia para usar. Tu app se puede eliminar si infringes las reglas y usas contenido sin permiso. Por supuesto, esto también significa que la app de otra persona se puede eliminar si esa persona la “tomó prestada” de tu trabajo. Si crees que otro desarrollador infringió tu propiedad intelectual en el App Store, envía un reclamo a través de nuestro [formulario web](#). Si bien las leyes difieren según el país o la región, te aconsejamos evitar al menos estos errores comunes:

5.2.1 En general: No uses material protegido de terceros, como marcas comerciales, trabajos protegidos por derechos de autor o ideas patentadas, en tu app sin permiso, y no incluyas afirmaciones, nombres o metadatos engañosos, falsos o copiados en el paquete de la app o el nombre del desarrollador. El envío de las apps debe estar a cargo de la persona o la entidad legal que sea titular o que tenga la licencia de la propiedad intelectual y otros derechos pertinentes.

5.2.2 Sitios o servicios de terceros: Si tu app usa, accede, monetiza el acceso o muestra contenido de un servicio de terceros, asegúrate de tener el permiso específico para hacerlo según los términos de uso del servicio. Se debe proporcionar autorización previa solicitud.

5.2.3 Descarga de audio o video: Las apps no deben facilitar el intercambio ilegal de archivos ni incluir la capacidad de guardar, convertir o descargar contenido multimedia de fuentes de terceros (p. ej., Apple Music, YouTube, SoundCloud, Vimeo, etc.) sin la autorización explícita de esas fuentes. La reproducción en streaming de contenido de audio o video también puede infringir los términos de uso, así que asegúrate de leerlos antes de que la app acceda a esos servicios. Se debe proporcionar autorización previa solicitud.

5.2.4 Respaldo de Apple:

(a)  No sugieras ni insinúes que Apple es la fuente o el proveedor de la app, ni que Apple respalda ninguna afirmación en particular con respecto a la calidad o la funcionalidad.

(b) Si tu app se selecciona como “Elección del editor”, Apple aplicará el distintivo automáticamente.

5.2.5 ➡ Productos Apple: No crees una app que se pueda confundir con otro producto, una interfaz (p. ej., el Finder), una app (como el App Store, iTunes Store o Mensajes) o un tema de publicidad existente de Apple. Las apps y las extensiones, como los paquetes de stickers y los teclados de terceros, no pueden incluir emojis de Apple. Las vistas previas de música de iTunes y Apple Music no se pueden usar para aprovechar su valor de entretenimiento (p. ej., como música de fondo de un collage de fotos o la banda sonora de un juego) ni de ninguna otra manera no autorizada. Si ofreces vistas previas de música de iTunes o Apple Music, debes proporcionar un enlace a la música correspondiente en iTunes o Apple Music. Si tu app muestra círculos de Actividad, estos no deben mostrar datos sobre cuánto te mueves, haces ejercicio y te paras de una forma similar al control de Actividad. En las [Human Interface Guidelines](#) se puede encontrar más información sobre cómo usar los círculos de Actividad. Si en tu app se muestran datos de Clima, debe seguir los requisitos de atribución que se indican en la [documentación de WeatherKit](#).

5.3 Juegos, apuestas y loterías

Los juegos, las apuestas y las loterías pueden ser difíciles de administrar y tienden a ser una de las ofertas más reguladas en el App Store. Solo incluye esta funcionalidad si revisaste todas las obligaciones legales de todos los lugares donde tu app esté disponible y si tienes todo preparado para dedicar tiempo adicional durante el proceso de revisión. Algunas cosas para tener en cuenta:

5.3.1 Los sorteos y los concursos deben estar patrocinados por el desarrollador de la app.

5.3.2 Las reglas oficiales para sorteos, concursos y rifas deben presentarse en la app y dejar en claro que Apple no patrocina ni participa de ninguna manera en la actividad.

5.3.3 Las apps no pueden usar la funcionalidad de compra dentro de la app para obtener crédito o dinero para usar en juegos que impliquen el uso de dinero real de cualquier tipo.

5.3.4 Las apps que ofrecen juegos con dinero real (p. ej., apuestas deportivas, póquer, juegos de casino, carreras de caballos) o loterías deben tener las licencias y los permisos necesarios en los lugares donde se usa la app, deben estar restringidas geográficamente a esas ubicaciones y deben ser gratuitas en el App Store. No se permiten ayudas para el juego ilegal, como los contadores de cartas, en el App Store. Las apps de lotería deben tener consideraciones, azar y un premio.

5.4 ➡ Apps de VPN

Las apps que ofrecen servicios de VPN deben usar la [API de NEVPNManager](#) y solo los desarrolladores que se hayan inscrito en una organización pueden ofrecerlas. Debes informar con claridad de qué datos del usuario se recopilarán y cómo se usarán en una pantalla de la app antes de que el usuario realice cualquier acción para comprar o usar de otro modo el servicio. Las apps que ofrecen servicios de VPN no pueden vender, usar ni divulgar a terceros ningún dato con ningún fin y deben comprometerse a no hacerlo en su política de privacidad. Las apps de VPN no deben infringir las leyes locales y, si eliges que tu app de VPN esté disponible en un territorio que requiere una licencia de VPN, debes proporcionar la información de la licencia en el campo de notas de App Review. Las apps de control parental, bloqueo de contenido y seguridad, entre otras, de proveedores aprobados también pueden usar la API de NEVPNManager. Las apps que no cumplan con este lineamiento se eliminarán del App Store y se

bloqueará su instalación a través de una distribución alternativa, y es posible que se te expulse de Apple Developer Program.

5.5 ➡ Administración de dispositivos móviles

Las apps de administración de dispositivos móviles que ofrecen servicios de administración de dispositivos móviles (MDM) deben solicitar esta capacidad a Apple. Estas apps solo pueden ser ofrecidas por empresas comerciales, instituciones educativas o agencias gubernamentales y, en casos limitados, empresas que usan MDM para ofrecer servicios de control parental o seguridad de dispositivos. Debes informar con claridad de qué datos del usuario se recopilarán y cómo se usarán en una pantalla de la app antes de que el usuario realice cualquier acción para comprar o usar de otro modo el servicio. Las apps de MDM no deben infringir ninguna ley aplicable. Las apps que ofrecen servicios de MDM no pueden vender, usar ni divulgar a terceros ningún dato con ningún fin y deben comprometerse a no hacerlo en su política de privacidad. En casos limitados, se pueden permitir análisis de terceros siempre que los servicios solo recopilen o transmitan datos sobre el rendimiento de la app de MDM del desarrollador, y no datos sobre el usuario, su dispositivo u otras apps usadas en ese dispositivo. Las apps que ofrecen perfiles de configuración también deben cumplir con estos requisitos. Las apps que no cumplan con este lineamiento se eliminarán del App Store y se bloqueará su instalación a través de una distribución alternativa, y es posible que se te expulse de Apple Developer Program.

5.6 ➡ Código de conducta para desarrolladores

Trata a todas las personas con respeto, ya sea en tus respuestas a las reseñas del App Store, las solicitudes de atención al cliente o cuando te comuniques con Apple, incluidas tus respuestas en App Store Connect. No te involucres en prácticas abusivas, discriminatorias, intimidatorias o agresivas de ningún tipo y tampoco incentives a otras personas a hacerlo. Los comportamientos manipuladores o engañosos reiterados u otras conductas fraudulentas darán como resultado la expulsión de Apple Developer Program.

La confianza del cliente es la piedra angular del ecosistema de apps. Las apps no deben aprovecharse de los usuarios ni tratar de estafar a clientes, engañarlos para que realicen compras no deseadas, forzarlos a compartir datos innecesarios, aumentar precios de manera engañosa, cobrar cargos por funcionalidades o contenido que no se entregan, ni involucrarse en ninguna otra práctica manipuladora dentro o fuera de la app.

Tu cuenta de Developer Program se dará de baja si participas en actividades o acciones que no se ajustan al Código de conducta para desarrolladores. Para restaurarla, puedes proporcionar una declaración por escrito que detalle las mejoras que planeas hacer. Si Apple aprueba tu plan y confirmamos que se realizaron los cambios, es posible que se restaure tu cuenta.

5.6.1 Reseñas del App Store

Las reseñas de los clientes del App Store pueden ser una parte integral de la experiencia de la app, por lo que debes tratar a los clientes con respeto al responder sus comentarios. Dirige tus respuestas a los comentarios del usuario y no incluyas en ellas información personal, spam o publicidad.

Usa la API proporcionada para pedirles a los usuarios que escriban una reseña sobre tu app. Esta funcionalidad les permite a los clientes proporcionar una calificación y una reseña en el App Store sin tener que salir de la app. No permitiremos solicitudes de reseñas personalizadas.

5.6.2 Identidad del desarrollador

Brindar información verificable tanto a Apple como a los clientes es fundamental para generar confianza. Tu representación, al igual que la de tu negocio y tus ofertas en el App Store o una plataforma de distribución alternativa, debe ser precisa. La información que proporcionas debe ser veraz, relevante y actualizada para que Apple y los clientes sepan con quién están tratando y puedan comunicarse contigo en caso de tener algún problema.

5.6.3 Detección de fraude

Participar en el App Store requiere integridad y el compromiso de generar y mantener la confianza de los clientes. La manipulación de cualquier elemento de la experiencia del cliente del App Store, como las listas, las búsquedas, las reseñas o las recomendaciones de tu app, deteriora la confianza del cliente y no está permitida.

5.6.4 Calidad de la app

Los clientes esperan la más alta calidad del App Store, y mantener contenido, servicios y experiencias de alta calidad promueve la confianza del cliente. Algunos indicadores que pueden mostrar que no se está cumpliendo esta expectativa pueden ser una cantidad excesiva de avisos de los clientes sobre inquietudes respecto de tu app, como reseñas negativas y demasiadas solicitudes de reembolso. La imposibilidad de mantener una alta calidad puede ser un factor para decidir si un desarrollador cumple con el Código de conducta para desarrolladores.

Después del envío

Una vez que hayas enviado la app y los metadatos a App Store Connect y estés en el proceso de revisión, debes tener en cuenta lo siguiente:

- **Tiempo:** App Review examinará tu app lo antes posible. Sin embargo, si tu app es compleja o presenta nuevos problemas, es posible que requiera un mayor escrutinio y consideración. Además, recuerda que si tu app se rechaza reiteradas veces por la misma infracción de los lineamientos o si intentaste manipular el proceso de revisión, la revisión de la app tardará más en completarse. Obtén más información sobre [App Review](#).
- **Actualizaciones de estado:** El estado actual de la app se reflejará en App Store Connect, de modo que podrás controlar todo desde allí.

- **Solicitudes de revisión acelerada:** Si tienes un problema importante con los tiempos, puedes [solicitar una revisión acelerada](#). Respeta a tus colegas desarrolladores y solicita una revisión acelerada solo cuando realmente la necesites. Si descubrimos que estás abusando de este sistema, es posible que rechacemos tus solicitudes en el futuro.
- **Fecha de lanzamiento:** Si tu fecha de lanzamiento está fijada para el futuro, la app no aparecerá en el App Store hasta esa fecha, incluso si App Review la aprueba. Además, recuerda que tu app puede tardar hasta 24 horas en aparecer en todas las tiendas seleccionadas.
- **Rechazos:** Nuestro objetivo es aplicar estos lineamientos de manera justa y coherente, pero sabemos que podemos equivocarnos. Si tu app fue rechazada y tienes preguntas o quieres proporcionar información adicional, usa App Store Connect para comunicarte directamente con el equipo de App Review. Esto puede permitir que tu app llegue a la tienda y puede ayudarnos a mejorar el proceso de App Review o identificar la necesidad de hacer aclaraciones en nuestras políticas.
- **Apelaciones:** Si no estás de acuerdo con el resultado de tu revisión, [envía una apelación](#). Esto puede permitir que tu app llegue a la tienda. También puedes [sugerir cambios en los lineamientos](#) para ayudarnos a mejorar el proceso de App Review o identificar la necesidad de hacer aclaraciones en nuestras políticas.
- **Envíos de correcciones de errores:** Para las apps que ya están en el App Store o en una distribución alternativa, las correcciones de errores no se demorarán por infracciones de los lineamientos, excepto las relacionadas con problemas legales o de seguridad. Si tu app fue rechazada y cumple los requisitos para este proceso, usa App Store Connect para comunicarte directamente con el equipo de App Review e indicar que quieres aprovechar este proceso para tratar de solucionar el problema en tu próximo envío.

Tenemos gran curiosidad por conocer tu próxima innovación.

Última actualización: [6 de febrero de 2026](#)