Directrices de App Review

Las apps están cambiando el mundo, enriqueciendo la vida de las personas y permitiendo a desarrolladores como tú innovar de una forma nunca vista antes. El resultado es que el App Store se ha convertido en un ecosistema fascinante y lleno de vida para millones de desarrolladores y más de mil millones de usuarios. Tanto si acabas de empezar en el mundo del desarrollo como si formas parte de un gran equipo de programadores experimentados, nos encanta saber que estás creando apps para nuestras plataformas y queremos que estés al tanto de nuestras directrices y así te asegures de que tu app supere rápidamente el proceso de revisión.

Noviembre de 2025

Introducción **4**
Antes del envío **5**
1. Seguridad **6**
1.1 Contenido inapropiado 6
1.2 Contenido generado por los usuarios 7
1.2.1 Contenido del creador 8
1.3 Categoría de niños 8
1.4 Daños físicos 9
1.5 Información para desarrolladores 9
1.6 Seguridad de los datos 10
1.7 Denuncia de actividad delictiva 10
2. Rendimiento **10**
2.1 Integridad de la app 10
2.2 Pruebas de versiones beta 10
2.3 Metadatos precisos 11
2.4 Compatibilidad de hardware 13
2.5 Requisitos de software 14
3. Empresas **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 19
3.1.2 (a) Usos permitidos 19
3.1.2 (b) Actualización o retroceso a una versión anterior 20
3.1.2 (c) Información de suscripción 20
3.1.3 Otros métodos de compra 20
3.1.3 (a) Apps de «lector» 20
3.1.3 (b) Servicios multiplataforma 21
3.1.3 (c) Servicios empresariales 21
3.1.3 (d) Servicios de persona a persona 21
3.1.3 (e) Bienes y servicios fuera de la app 21
3.1.3 (f) Apps independientes gratuitas 21
3.1.3 (g) Apps de gestión de publicidad 21
3.1.4 Contenido específico del hardware 22
3.1.5 Criptomonedas 22
3.2 Otros problemas del modelo empresarial 22
3.2.1 Aceptable 23

3.2.2 Inaceptable 23
4. Diseño **24**
4.1 Imitaciones 25
4.2 Funcionalidad mínima 25
4.2.7 Clientes de escritorio remoto 26
4.3 Spam 26
4.4 Extensiones 26
4.5 Sitios y servicios de Apple 27
4.6 Omisión intencionada. 29
4.7 Miniapps, minijuegos, juegos en streaming, chatbots, módulos y emuladores de juegos 29
4.8 Servicios de inicio de sesión 29
4.9 Apple Pay 30
4.10 Monetizar las capacidades integradas 31
5. Aspectos legales **31**
5.1 Privacidad 31
5.1.1 Recopilación y almacenamiento de datos 31
5.1.2 Uso e intercambio de datos 33
5.1.3 Salud e investigación sanitaria 34
5.1.4 Niños 35
5.1.5 Servicios de localización 35
5.2 Propiedad intelectual 36
5.3 Juegos, apuestas y loterías 37
5.4 Apps con red privada virtual (VPN) 37
5.5 Gestión de dispositivos móviles 37
5.6 Código de conducta para desarrolladores 38
5.6.1 Reseñas del App Store 38
5.6.2 Identidad del desarrollador 38
5.6.3 Fraude de descubrimiento 39
5.6.4 Calidad de la app 39
Después del envío **39**

Introducción

El principio que guía al App Store es sencillo: queremos ofrecer a los usuarios una experiencia segura a la hora de obtener apps y una gran oportunidad para que todos los desarrolladores tengan éxito. Para ello, ofrecemos un App Store con una selección cuidada de contenido, donde cada app es revisada por expertos, y un equipo editorial ayuda a los usuarios a descubrir nuevas apps todos los días. También escaneamos cada una de las apps en busca de malware y otro software que pueda afectar a la seguridad y privacidad del usuario. Estos esfuerzos han hecho que las plataformas de Apple sean las más seguras de todo el mundo para los consumidores.

En la Unión Europea, los desarrolladores también pueden distribuir apps iOS y iPadOS certificadas ante notario desde mercados de apps alternativos y directamente desde su sitio web. Obtén más información sobre los mercados de apps alternativos, la distribución web y la notarización de apps de iOS y iPadOS. Puedes ver qué directrices se aplican a la notarización de apps de iOS y iPadOS haciendo clic en «Mostrar solo Directrices de revisión de notarización» en el menú de la izquierda.

Para todo lo demás, siempre está la opción de internet. Si el modelo y las directrices del App Store (o los métodos de distribución alternativos y la notarización de apps de iOS y iPadOS) no son los más óptimos para tu app o idea de negocio, también tienes Safari, que te permitirá disfrutar de una fantástica experiencia web.

En las siguientes páginas, encontrarás nuestras directrices más recientes organizadas en cinco secciones bien definidas: Seguridad, Rendimiento, Negocio, Diseño y Aspectos legales. El App Store cambia y mejora constantemente para satisfacer las necesidades de nuestros clientes y nuestros productos. De la misma forma, tus apps deberían cambiar y mejorar para permanecer en el App Store.

Hay otros puntos que debes tener en cuenta a la hora de distribuir tu app en nuestras plataformas:

• Muchas personas menores de edad descargan nuestras apps. Los controles parentales funcionan muy bien para proteger a los menores, pero tú también tienes que poner tu granito de arena. Así que ten en cuenta que siempre pensamos en ellos.

• 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 mostrar a familiares y amistades, el App Store no es la mejor opción. Considera la opción de usar Xcode para instalar tu app en un dispositivo de forma gratuita o usar la distribución Ad Hoc disponible para los miembros del Apple Developer Program. Si estás dando tus primeros pasos en este ámbito, obtén más información sobre el Apple Developer Program.

• Apoyamos firmemente todos los puntos de vista que se representan en el App Store, siempre y cuando las apps respeten a los usuarios con opiniones diferentes y la calidad de la experiencia de la app sea excelente. Rechazaremos las apps que contengan cualquier contenido o comportamiento que creamos que esté fuera de lugar. ¿En qué nos basamos para esto? Como dijo una vez un juez del Tribunal Supremo: «Lo sabré cuando lo vea». Creemos que tú también lo sabrás cuando te encuentres con algo así.

• Si intentas engañar al sistema (por ejemplo, haciendo trampas en el proceso de revisión, robando datos de usuario, copiando el trabajo de otro desarrollador o manipulando las calificaciones o el método de descubrimiento de apps del App Store), tus apps se eliminarán de la tienda y se te expulsará del Apple Developer Program.

• Tienes la responsabilidad de asegurarte de que todo el contenido de tu app cumpla con estas directrices, incluidos los servicios de análisis, los kits de desarrollo de software (SDK) de otros fabricantes y las redes publicitarias, así que revisa y selecciona todos estos elementos con atención.

• Algunas prestaciones y tecnologías que generalmente no están disponibles para los desarrolladores pueden ofrecerse como autorización para casos de uso limitados. Por ejemplo, ofrecemos autorizaciones para CarPlay Audio, HyperVisor y Privileged File Operations.

Esperamos que estas directrices te ayuden a superar el proceso de revisión y que faciliten también un sistema coherente para aprobar y rechazar propuestas en todo el entorno. Este documento puede cambiar en cualquier momento. Existe la posibilidad de que las nuevas apps que plantean nuevas preguntas generen reglas nuevas. Quizás tu app sea una de ellas. Nos gusta que ocurran estas cosas, y admiramos mucho lo que haces. No dudes de que estamos haciendo todo lo posible para crear la mejor plataforma del mundo donde puedas expresar tu talento y obtener beneficios también.

Antes del envío

Para facilitar el proceso de aprobación de apps, echa un vistazo a los errores comunes que suelen surgir durante la revisión. Esta lista no pretende reemplazar las directrices ni supone una garantía de aprobación, pero comprobar cada uno de sus puntos es un buen comienzo. Si tu app ha dejado de funcionar correctamente o ya no ofreces soporte para ella de forma activa, se eliminará del App Store. Obtén más información sobre las mejoras del App Store.

Asegúrate de:

- Probar tu app en busca de fallos y errores.
- Garantizar que toda la información y los metadatos de la app estén completos y sean precisos.
- Actualizar tu información de contacto en caso de que App Review necesite contactar contigo.
- Proporcionar a App Review acceso completo a tu app. Si tu app incluye prestaciones basadas en cuentas, proporciona una cuenta de demostración activa o un modo de demostración con todas las prestaciones, además de cualquier otro hardware o recurso que pueda ser necesario para revisar la app (por ejemplo, credenciales de inicio de sesión o un código QR de muestra).
- Habilitar servicios back-end para que estén activos y accesibles durante la revisión.
- Incluir en las notas para App Review explicaciones detalladas sobre prestaciones que no son obvias y compras dentro de la app, incluida cualquier documentación complementaria cuando proceda.
- Comprobar si tu app sigue las instrucciones de otra documentación, como:

Documentación para desarrolladores

- SwiftUI
- UIKit
- AppKit
- Extensiones de apps
- Optimizar los datos de tu app para la copia de seguridad en iCloud
- Apple File System
- Ayuda de App Store Connect
- Ayuda de cuenta de desarrollador

Directrices de diseño

- Directrices de interfaz humana

Directrices de marca y marketing

- Recursos de marketing y directrices de identidad
- Directrices de marketing de Apple Pay
- Directrices para añadir contenido a Cartera
- Directrices de uso de marcas comerciales y derechos de autor de Apple

Las directrices que incluyen 🕶 se aplican a la notarización de apps de iOS y iPadOS en la UE.

---

1. Seguridad

Cuando alguien instala una app desde el App Store, lo hace confiando en su seguridad; es decir, en que la app no incluye contenido desagradable ni ofensivo, no dañará su dispositivo y es improbable que cause daños físicos al usarla. Hemos descrito los principales inconvenientes, pero si lo que pretendes es consternar y ofender a los usuarios, el App Store no es el mejor lugar para tu app. Algunas de estas reglas también se incluyen en Notarización de apps de iOS y iPadOS.

1.1 Contenido inapropiado

Las apps no deben incluir contenido que sea ofensivo, desconsiderado, desagradable, creado con la intención de indignar o que sea simplemente inquietante. Algunos ejemplos de este tipo de contenido son:

1.1.1 Contenido difamatorio, discriminatorio o malintencionado, incluidas referencias o comentarios sobre cuestiones relacionadas con la religión, la raza, la orientación sexual, el género, el origen nacional o étnico, u otros grupos objetivo, en particular si supone una fuente de humillación o intimidación, o un peligro para un grupo o una persona en concreto. Los humoristas y escritores satíricos profesionales están, por lo general, exentos de este requisito.

1.1.2 Retratos realistas de personas o animales que estén siendo asesinados, mutilados, torturados o de los que se esté abusando. Tampoco se permite contenido que anime a practicar la violencia. Los «enemigos» dentro del contexto de un juego no pueden pertenecer en exclusividad a una raza, cultura, gobierno, corporación u otra entidad real determinada.

1.1.3 Descripciones que inciten a usar de forma ilegal o temeraria armas y objetos peligrosos, o bien que faciliten la compra de armas de fuego o munición.

1.1.4 Material que sea explícitamente sexual o pornográfico, definido como «muestras o descripciones explícitas de órganos sexuales o actividades que pretendan estimular las sensaciones eróticas en lugar de las estéticas o las emocionales». Esto incluye apps de «citas» y otras apps que puedan incluir pornografía o utilizarse para facilitar la prostitución o la trata y explotación de personas.

1.1.5 Comentarios religiosos con los que se pretenda provocar, o bien citas imprecisas o engañosas de textos religiosos.

1.1.6 🕶 Prestaciones e información falsas, incluidos datos imprecisos sobre dispositivos o funcionalidades trampa o de broma, como rastreadores de ubicación falsos. En este caso, declarar que la app tiene «fines de entretenimiento» no servirá para ignorar esta instrucción. Se rechazarán las apps que permitan realizar llamadas anónimas o falsas, o enviar mensajes SMS/MMS de este tipo.

1.1.7 Conceptos nocivos que aprovechan o buscan sacar provecho de acontecimientos recientes o actuales, como conflictos violentos, ataques terroristas y epidemias.

1.2 Contenido generado por los usuarios

Las apps con contenido generado por los usuarios presentan retos muy particulares que van desde la vulneración de los derechos de propiedad intelectual al hostigamiento anónimo. Para evitar abusos, las apps con contenido generado por los usuarios o los servicios de redes sociales deben incluir:

- Un método para filtrar el material inapropiado y evitar que se publique en la app.
- Un mecanismo para denunciar el contenido ofensivo y ofrecer una respuesta rápida a los problemas.
- La capacidad de bloquear a los usuarios que usen el servicio de forma indebida.
- Información de contacto publicada para que los usuarios puedan contactar contigo.

Las apps con servicios o contenido generado por los usuarios que acaben siendo utilizadas principalmente para mostrar contenido pornográfico, ofrecer experiencias tipo Chatroulette, deshumanizar a personas reales (por ejemplo, las votaciones del tipo «hot-or-not»), realizar amenazas físicas o acosar no pueden permanecer en el App Store y se podrían eliminar sin aviso previo. Si tu app incluye contenido generado por los usuarios a partir de un servicio basado en web, podría mostrar contenido fortuito «NSFW» (no apto para verlo en el trabajo) para personas adultas, siempre que esté oculto por defecto y solo se muestre cuando el usuario lo active en tu sitio web.

1.2.1 Contenido del creador

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 ayudar a esta comunidad de creadores no desarrolladores a crear, compartir y monetizar experiencias generadas por los usuarios. Estas experiencias no deben cambiar las prestaciones y la funcionalidad principales de la app nativa; lo que hacen es añadir contenido a esas experiencias estructuradas. Estas experiencias no son «apps» nativas codificadas por los desarrolladores, sino contenido de la propia app, y App Review las trata como contenido generado por los usuarios. Este tipo de contenido puede incluir vídeos, artículos, audio e incluso juegos casuales. El App Store admite apps que ofrezcan dicho contenido generado por los usuarios siempre que sigan todas las directrices, incluida la Directriz 1.2 para moderar el contenido generado por los usuarios y la Directriz 3.1.1 sobre pagos y compras dentro de la app. Debes comunicar a los usuarios qué contenido requiere compras adicionales.

(a) Las apps para creadores deben ofrecer a los usuarios una forma de identificar el contenido que supere la clasificación por edades de la app y utilizar un mecanismo de restricción por edad basado en la edad verificada o declarada para limitar el acceso de los usuarios menores de edad.

1.3 Categoría de niños

La categoría de niños es una forma estupenda de encontrar fácilmente apps diseñadas para los pequeños de la casa. Si quieres participar en la categoría de niños, debes centrarte en crear una gran experiencia específicamente para los usuarios más jóvenes. Estas apps no deben incluir enlaces que dirijan a sitios fuera de la app, oportunidades de compra ni otro contenido que pueda distraer a los niños, a menos que estén reservados a un área específica de control parental. Ten en cuenta que, una vez que los clientes esperen que tu app siga los requisitos de esta categoría, las siguientes actualizaciones tendrán que acogerse a estas directrices, incluso si decides anular la selección de esta categoría. Obtén más información sobre el control parental.

Debes cumplir las leyes de privacidad aplicables en todo el mundo relacionadas con la recopilación en línea de datos de niños. Asegúrate de revisar la sección Privacidad de estas directrices para obtener más información. Además, las apps de la categoría de niños no pueden enviar información de identificación personal ni información del dispositivo a terceros. Las apps de la categoría de niños no deben incluir análisis ni publicidad de otros fabricantes. Esto proporciona 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 ninguna información identificable sobre los niños (como el nombre, la fecha de nacimiento o la dirección de correo electrónico), su ubicación o sus dispositivos. Esto incluye 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 otros fabricantes también puede permitirse en casos limitados, siempre que los servicios cuenten con prácticas y políticas públicamente documentadas para las apps de la categoría de niños que incluyan la revisión humana de los mensajes publicitarios con el fin de verificar su idoneidad para la edad.

1.4 Daños físicos

Podemos rechazar la app si presenta riesgos de daños físicos. Por ejemplo:

1.4.1 Las apps médicas que podrían proporcionar información o datos imprecisos, o bien aquellas que sirven para diagnosticar o tratar a pacientes, se revisarán con mayor exhaustividad.

• Las apps deben presentar de forma clara la información y la metodología que respaldan las declaraciones relativas a la precisión de los datos de salud. En caso de que no sea posible validar el nivel de precisión o la metodología, rechazaremos tu app. Por ejemplo, no se admiten las apps diseñadas para hacer radiografías o medir la presión sanguínea, la temperatura corporal, el nivel de glucosa en sangre o el nivel de oxígeno en sangre que solo utilicen los sensores del dispositivo.

• Las apps deben recordar a los usuarios que también es conveniente consultar a un médico antes de tomar decisiones que puedan afectar a su salud.

Si tu app médica cuenta con la autorización reglamentaria, envía un enlace a esa documentación junto con la app.

1.4.2 Las calculadoras de dosis de fármacos deben provenir de fabricantes de medicamentos, hospitales, universidades, compañías de seguros sanitarios, farmacias u otras entidades aprobadas. Otra alternativa es que la FDA o uno de sus homólogos internacionales las haya aprobado. Dado el posible daño que se puede causar a los pacientes, tenemos que estar seguros de que la app contará con soporte y actualizaciones a largo plazo.

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

1.4.4 Las apps solo pueden mostrar los controles de alcoholemia que publiquen las fuerzas y cuerpos de seguridad, y nunca pueden incitar a conducir bajo los efectos del alcohol u otras conductas temerarias, como el exceso de velocidad.

1.4.5 Las apps no deben instar a los clientes a participar en actividades (como apuestas, desafíos, etc.) o usar sus dispositivos de manera que puedan causar daños físicos a ellos mismos o a otros.

1.5 Información para desarrolladores

Es necesario indicar cómo es posible localizarte en caso de tener dudas y problemas de soporte técnico. Asegúrate de que tu app y su URL para el soporte técnico incluyan una forma fácil de contactar contigo; esto es especialmente importante para las apps que se pueden usar en el aula. No incluir información de contacto precisa y actualizada no solo frustra a los clientes, sino que puede infringir la ley en algunos países o regiones. Asimismo, asegúrate de que los pases de Cartera incluyan información de contacto válida del emisor y de que estén firmados con un certificado dedicado que se haya asignado al titular de la marca o marca comercial del pase.

1.6 Seguridad de los datos

Las apps deben implementar medidas de seguridad adecuadas para garantizar el manejo adecuado de la información del usuario recopilada de conformidad con el Contrato de Licencia del Apple Developer Program y estas Directrices (consulta la Directriz 5.1 para obtener más información) y evitar su uso, divulgación o acceso no autorizados por parte de terceros.

1.7 Denuncia de actividad delictiva

Las apps para denunciar una presunta actividad delictiva deben involucrar a las autoridades locales y solo se pueden ofrecer en países o regiones donde dicha participación esté activa.

---

2. Rendimiento

2.1 Integridad de la app

(a) Los envíos a App Review, incluidas las apps que pongas a disposición para pedidos por adelantado, deben ser versiones finales, con todos los metadatos necesarios y las URL completamente funcionales incluidas. Los marcadores de posición de texto, los sitios web vacíos y otros contenidos temporales deben borrarse antes del envío. Confirma que la app se ha probado en dispositivos para comprobar su estabilidad y que no quedan errores antes de enviarla. Incluye también la información de una cuenta de demostración (y activa el servicio de back-end) si la app incluye un inicio de sesión. Si no puedes proporcionar una 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 el modo de demostración muestre todas las prestaciones y la funcionalidad de tu app. Rechazaremos los paquetes de apps incompletos y los binarios que se bloqueen o presenten problemas técnicos evidentes.

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

2.2 Pruebas de versiones beta

No se aceptan versiones de demostración, beta y de prueba de la app en el App Store; utiliza TestFlight para ello. Las apps que se envíen para la distribución de su versión beta a través de TestFlight se deben destinar a la distribución pública y deben cumplir las Directrices de App Review. Ten en cuenta, sin embargo, que las apps que utilizan TestFlight no se pueden enviar a los controladores de calidad a cambio de compensaciones de ningún tipo, incluidas las recompensas que se obtengan a través de actividades de microfinanciación colectiva. Las actualizaciones significativas de la versión beta se deben enviar a TestFlight App Review antes de distribuirlas a los controladores de calidad. Para obtener más información, visita la página Pruebas de versiones beta en TestFlight.

2.3 Metadatos precisos

Los clientes deben saber qué van a obtener cuando descarguen o compren la app; por ello es muy importante que la descripción, las capturas de pantalla y las vistas previas que la acompañan reflejen de forma precisa su experiencia principal. Es igualmente fundamental que las actualices con cada nueva versión.

2.3.1

(a) No incluyas ninguna prestación oculta, inactiva o indocumentada en tu app; la funcionalidad de tu app debe ser clara para los usuarios finales y App Review. Todas las nuevas prestaciones, funcionalidades y cambios de productos deben describirse con detalle en la sección Notas para revisión de App Store Connect (se rechazarán las descripciones genéricas) y deben ser accesibles para su revisión. Del mismo modo, promocionar tu app de forma engañosa, como promocionar contenido o servicios que en realidad no se ofrecen (por ejemplo, un escáner de software dañino y virus basado en iOS) o promocionar un precio falso, ya sea dentro o fuera del App Store, es motivo para eliminarla del App Store, bloquear su instalación mediante métodos de distribución alternativos y cancelar tu cuenta de desarrollador.

(b) Los comportamientos repetidos o indignantes son motivo de expulsión del Apple Developer Program. Nos esforzamos mucho para garantizar que el App Store sea un ecosistema de confianza y esperamos que nuestros desarrolladores de apps sigan nuestro ejemplo. Si actúas de forma deshonesta, no queremos hacer tratos contigo.

2.3.2 Si incluyes compras dentro de la app, asegúrate de que la descripción, las capturas de pantalla y las vistas previas indiquen claramente si algún elemento, nivel, suscripción, etc. requiere compras adicionales. Si decides promocionar las compras dentro de la app en el App Store, asegúrate de que su nombre visible, la captura de pantalla y su descripción sean adecuados para el público objetivo general, que sigues las instrucciones que se encuentran en Promocionar tus compras dentro de la app y que tu app gestiona adecuadamente el método SKPaymentTransactionObserver, de modo que los clientes puedan realizar la compra sin problemas cuando tu app pase a estar disponible.

2.3.3 Las capturas de pantalla deben mostrar la app en uso y no solo el título, la página de inicio de sesión o la pantalla de inicio. También pueden incluir texto e imágenes superpuestos (por ejemplo, para presentar mecanismos de entrada como un punto de contacto animado o un Apple Pencil), o mostrar otras funciones del dispositivo, como la Touch Bar.

2.3.4 Las vistas previas constituyen una forma fantástica para que los clientes puedan ver el aspecto que tiene la app y lo que hace. Para estar seguros de que los clientes comprenden lo que van a obtener con la app, es posible utilizar capturas de pantalla en vídeo de la propia app como vistas previas. Los stickers y las extensiones de iMessage pueden mostrar la experiencia del usuario en la app Mensajes. Puedes añadir narración y vídeo o superposiciones de texto para ayudar a explicar cualquier cosa que no esté clara solo en el vídeo.

2.3.5 Selecciona la categoría más adecuada para tu app y comprueba las definiciones de categorías del App Store si necesitas ayuda. Si te equivocas, podríamos cambiar la categoría por ti.

2.3.6 Responde honestamente a las preguntas de clasificación por edades en App Store Connect para que tu app se alinee correctamente con los controles parentales. Si esta clasificación no se realiza bien, el contenido de lo que obtienen los clientes podría sorprenderles o las autoridades gubernamentales podrían comenzar una investigación al respecto. Si tu app incluye contenido multimedia que requiere que se muestren advertencias o clasificaciones de contenido (por ejemplo, películas, música, juegos, etc.), eres responsable de cumplir los requisitos locales en cada territorio donde tu app esté disponible.

2.3.7 Elige un nombre exclusivo para la app, asigna palabras clave que la describan con precisión y no intentes unir los metadatos con términos de marcas comerciales, nombres de app populares u otras frases irrelevantes para intentar engañar al sistema. Los nombres de las apps deben tener un límite de 30 caracteres. Los metadatos, como los nombres de las apps, los subtítulos, las capturas de pantalla y las vistas previas, no deben incluir precios, términos o descripciones que no sean específicos del tipo de metadatos. Los subtítulos son una forma fantástica de ampliar la información sobre tu app. Estos deben seguir nuestras reglas estándar para metadatos y no pueden incluir contenido inapropiado, referencias a otras apps ni afirmaciones sobre productos que no se puedan verificar. Apple puede modificar las palabras clave inapropiadas en cualquier momento o tomar otras medidas adecuadas para evitar abusos.

2.3.8 Los metadatos deben ser apropiados para todos los públicos, por lo que debes asegurarte de que los iconos, capturas de pantalla y vistas previas de tu app y de las compras dentro de la app sean adecuados para edades a partir de los 4 años, incluso si la app está destinada a un público de más edad. Por ejemplo, si la app es un juego que incluye violencia, selecciona imágenes que no representen una muerte espantosa ni muestren una pistola apuntando a un personaje determinado. El uso de términos como «Para niños» y «Para menores» en los metadatos de apps está reservado en el App Store a la categoría de niños. Debes asegurarte de que los metadatos, incluidos el nombre y los iconos de la app (pequeño, grande, la app Watch, iconos alternativos, etc.), sean similares para no crear confusión.

2.3.9 Eres responsable de garantizar los derechos para poder usar todos los materiales de iconos, capturas de pantalla y vistas previas de la app, y debes mostrar información de una cuenta ficticia en lugar de datos de personas reales.

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

2.3.11 Las apps que envíes para reserva en el App Store deben estar completas y entregarse tal como se envían. Asegúrate de que la app que publiques no sea sustancialmente diferente de lo que anuncias mientras la app está en un estado de reserva. Si haces cambios importantes en la app (por ejemplo, cambias los modelos de negocio), debes reiniciar las reservas.

2.3.12 Las apps deben describir claramente las nuevas prestaciones y los cambios del producto en el texto «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 significativos deben enumerarse en las notas.

2.3.13 Los eventos dentro de la app son eventos puntuales que ocurren dentro de tu app. Para presentar tu evento 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 pertenecer al evento en sí, en lugar de a la app en general. Los eventos deben realizarse en las fechas y horas que selecciones en App Store Connect, incluso en varias tiendas. Puedes monetizar tu evento siempre que sigas las reglas establecidas en la Sección 3 en Empresas. Además, el enlace directo de tu evento debe dirigir a los usuarios al destino adecuado dentro de tu app. Lee Eventos dentro de la app para obtener directrices detalladas sobre los metadatos de eventos aceptables y los enlaces directos de eventos.

2.4 Compatibilidad de hardware

2.4.1 Para que las personas aprovechen al máximo tu app, las apps del iPhone deben ejecutarse en el iPad siempre que sea posible. Te animamos a que consideres la posibilidad de crear apps para que los clientes puedan usarlas en todos sus dispositivos.

2.4.2 Diseña tu app para que utilice la energía de forma eficiente y sin riesgo de dañar el dispositivo. Las apps no deben agotar rápidamente la batería, generar un calor excesivo o hacer un uso innecesario de los recursos de los dispositivos. Por ejemplo, las apps no deben recomendar que se coloque el dispositivo debajo de un colchón o una almohada mientras se carga ni realizar demasiados ciclos de escritura en la unidad de estado sólido. Las apps, incluidos los anuncios de otros fabricantes que se muestran en ellas, no pueden ejecutar procesos en segundo plano no relacionados, como la minería de criptomonedas.

2.4.3 Las personas deben poder usar la app del Apple TV sin la necesidad de utilizar otras entradas de hardware que no sean las del mando Siri Remote o mandos de otros fabricantes. No obstante, si quieres, puedes proporcionar una mejor funcionalidad cuando se conecten otros periféricos. Si es necesario utilizar un mando, asegúrate de explicarlo claramente en los metadatos para que los clientes sepan que necesitan otros dispositivos para poder jugar.

2.4.4 Las apps nunca deben sugerir o requerir un reinicio del dispositivo o modificaciones en los ajustes del sistema que no estén relacionadas con la funcionalidad principal de la app. Por ejemplo, no animes a los usuarios a desactivar el wifi, las prestaciones de seguridad, etc.

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

(i) Deben estar en una zona protegida adecuada y seguir la documentación del sistema de archivos macOS. También deben usar únicamente las interfaces de programación de aplicaciones (API) de macOS apropiadas para modificar los datos del usuario que almacenan otras apps (por ejemplo, los marcadores y las entradas de la Agenda o del Calendario).

(ii) Se deben empaquetar y enviar con las tecnologías que se proporcionan en Xcode; no se permiten instaladores de otros fabricantes. También deben ser paquetes de instalación de apps sencillos y autónomos, y no pueden instalar códigos o recursos en ubicaciones compartidas.

(iii) No pueden iniciarse de forma automática ni tener otro código que se ejecute automáticamente durante el arranque o el inicio de sesión sin consentimiento, ni inicios de procesos que se sigan ejecutando sin consentimiento una vez que el usuario haya salido de la app. No deben añadir automáticamente iconos al Dock ni crear accesos directos en el escritorio del usuario.

(iv) No deben descargar ni instalar apps independientes, KEXT, código adicional o recursos que añadan funcionalidades o cambien significativamente la app con respecto a lo que vemos durante el proceso de revisión.

(v) No deben solicitar el escalado de privilegios de root o usar atributos setuid.

(vi) No deben mostrar una pantalla de licencia al iniciarse, pedir claves de licencia o implementar su propia protección contra copias.

(vii) Deben utilizar el Mac App Store para distribuir actualizaciones; no se permiten otros mecanismos de actualización.

(viii) Las apps se deben ejecutar en el sistema operativo actual y no deben usar tecnologías obsoletas o instaladas de manera opcional (por ejemplo, Java).

(ix) Las apps deben contener todos los idiomas y soporte de localización en un único paquete.

2.5 Requisitos de software

2.5.1 Las apps solo pueden utilizar API públicas y se deben ejecutar en el sistema operativo actual. Obtén más información sobre las API públicas. Actualiza tus apps y asegúrate de que eliminas las prestaciones, entornos y tecnologías obsoletas que no serán compatibles con las próximas versiones de un sistema operativo. Las apps deben usar API y marcos para los fines que persigan, así como indicar esa integración en la descripción que hagan de ella. Por ejemplo, en el marco de HomeKit se deben proporcionar servicios de automatización para el hogar, y HealthKit se debe usar para fines relacionados con la salud y el bienestar físico, y se debe integrar con la app Salud.

2.5.2 Las apps deben tener todo lo necesario en los paquetes y no deben leer ni escribir datos fuera del área del contenedor designada. Tampoco deben descargar, instalar o ejecutar código que introduzca o cambie prestaciones o funcionalidad de la app, incluidas otras apps. Las apps educativas diseñadas para enseñar o desarrollar código ejecutable, o para permitir que los estudiantes lo prueben, pueden descargar código en determinadas circunstancias, siempre que dicho código no se utilice para otros fines. Estas apps deben mostrar el código fuente que proporciona la app de forma totalmente visible y permitir que el usuario lo edite.

2.5.3 Se rechazarán las apps que transmitan virus, archivos, código informático o programas que puedan dañar o interrumpir el funcionamiento normal del sistema operativo y las prestaciones de hardware, incluidas las notificaciones push y el Game Center. Las violaciones flagrantes y los comportamientos repetidos provocarán la eliminación del Apple Developer Program.

2.5.4 Las apps multitarea solo pueden usar servicios en segundo plano para los fines pretendidos: VoIP, reproducción de audio, ubicación, finalización de tareas, notificaciones locales, etc.

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

2.5.6 Las apps que naveguen por la red deben utilizar el entorno WebKit y JavaScript de WebKit. Puedes solicitar la autorización para usar en tu app un motor de navegador web alternativo. Obtén más información sobre esta autorización.

2.5.7 Omisión intencionada.

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 deshabiliten las funciones de los interruptores estándar, como los interruptores para subir/bajar el volumen y los de timbre/silencio, u otros elementos o comportamientos nativos de la interfaz de usuario. Por ejemplo, las apps no deben bloquear enlaces a otras apps o a prestaciones que los usuarios esperan que funcionen de una manera determinada.

2.5.10 Omisión intencionada.

2.5.11 SiriKit y atajos

> **(i)** Las apps que integran SiriKit y atajos solo deben registrar intenciones que puedan gestionar sin la ayuda de otra app y que se correspondan con las expectativas de los usuarios en relación con la funcionalidad manifiesta. Por ejemplo, si tu app sirve para planificar las comidas, no debes incorporar una intención para iniciar 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 (plist) están relacionadas con tu app y la funcionalidad de las intenciones de Siri para las que se ha registrado la app. Los alias deben estar relacionados directamente con el nombre de tu empresa o tu app y no deben ser términos genéricos ni incluir servicios o nombres de apps de otros fabricantes.
>
> **(iii)** Resuelve la solicitud o el atajo de Siri de la forma más directa posible y no insertes anuncios u otro material de marketing entre la solicitud y su cumplimiento. Solicita una desambiguación únicamente cuando sea necesaria para completar la tarea (por ejemplo, pedir al usuario que especifique un tipo determinado de entrenamiento).

2.5.12 Las apps que usan CallKit o incluyen una extensión para evitar fraudes por SMS solo deben bloquear los números de teléfono que se han confirmado como spam. Las apps que incluyen una funcionalidad de bloqueo de llamadas, SMS y MMS o identificación de spam deben mencionar claramente dichas prestaciones en el texto de marketing e indicar los criterios que usan en sus listas de spam o números bloqueados. No puedes usar los datos disponibles a través de estas herramientas para fines que no estén directamente relacionados con el funcionamiento o la mejora de tu app o extensión (por ejemplo, no puedes usarlos, compartirlos ni venderlos para realizar seguimientos, crear perfiles de usuario, etc.).

2.5.13 Las apps que utilicen el reconocimiento facial para la autenticación de cuentas deben usar LocalAuthentication (y no ARKit u otra tecnología de reconocimiento facial) y contar con otro método de autenticación 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 audible clara al grabar, iniciar sesión o hacer un registro de la actividad del usuario. Esto incluye cualquier uso de la cámara del dispositivo, el micrófono, las grabaciones de pantalla u otras acciones 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 estar relacionados con el contenido y la funcionalidad de tu app.

(a) Además, todas las prestaciones y funciones del clip de app deben incluirse en el binario principal de la app. Los clips de apps no pueden contener publicidad.

2.5.17 Las apps compatibles con Matter deben usar el marco de soporte de Apple para que Matter inicie el emparejamiento. Además, si eliges usar cualquier componente de software de Matter en una app que no sea el SDK de Matter proporcionado por Apple, el componente de software debe estar certificado por la Alianza de Estándares de Conectividad para la plataforma en la que se ejecuta.

2.5.18 La publicidad gráfica debe limitarse al archivo binario principal de la app y no debe incluirse en extensiones, clips de apps, widgets, notificaciones, teclados, apps de watchOS, etc. Los anuncios que se muestran en una app deben ser adecuados para la clasificación por edades de la app, permitir al usuario ver toda la información utilizada para orientarlo a ese anuncio (sin que el usuario tenga que abandonar la app) y no pueden participar en publicidad basada en datos confidenciales del usuario dirigida o basada en el comportamiento, como datos de salud/médicos (por ejemplo, de las API de HealthKit), datos de la escuela y el aula (por ejemplo, de ClassKit) o de niños (por ejemplo, de apps de la categoría de niños del App Store), etc. Los anuncios intersticiales o los anuncios que interrumpen o bloquean la experiencia del usuario deben indicar claramente que son un anuncio, no deben manipular ni engañar a los usuarios para que los pulsen, y deben proporcionar botones de cierre/omisión fácilmente accesibles y visibles lo suficientemente grandes para que las personas puedan ignorarlos fácilmente. Las apps que contienen anuncios también deben incluir la capacidad de que los usuarios informen de anuncios inapropiados o no aptos para ciertas edades.

---

3. Empresas

Hay muchas formas de monetizar tu app en el App Store. Si tu modelo de negocio no es obvio, asegúrate de explicarlo en sus metadatos y notas de App Review. Si no podemos comprender cómo funciona la app o las compras dentro de esta no son obvias de manera inmediata, supondrá un retraso en el proceso de revisión y podría originar un rechazo. Y, si bien el precio es una cuestión que solo depende de ti,

no distribuiremos apps y artículos de compras dentro de apps que sean claramente una estafa. Rechazaremos apps caras que intenten engañar a los usuarios con precios desorbitados.

Si nos percatamos de que estás intentando manipular las revisiones, inflar las clasificaciones con comentarios pagados, incentivados, filtrados o falsos, o bien que hayas contratado servicios de otros fabricantes para que lo hagan por ti, tomaremos las medidas oportunas para conservar la integridad del App Store, lo que puede suponer tu expulsión del Apple Developer Program.

3.1 Pagos

3.1.1 Compras dentro de la app

- Si quieres desbloquear prestaciones o funcionalidades dentro de tu app, (a modo de ejemplo: suscripciones, divisas que se usan en los juegos, niveles de los juegos, acceso a contenido premium o desbloqueo de una versión completa), debes utilizar las compras dentro de la app. Las apps no deben usar sus propios mecanismos para desbloquear contenido o funcionalidades, como claves de licencia, marcadores de realidad aumentada, códigos QR, criptomonedas y carteras de criptomonedas, etc.

- Las apps pueden usar las divisas de compras dentro de la app para permitir a los clientes dar propina a los desarrolladores o proveedores de contenido digital de la app.

- Los créditos y las divisas para los juegos que se adquieren a través de las compras dentro de las apps no pueden caducar. Además, debes asegurarte de que dispones de un mecanismo de restauración para las compras dentro de la app que se puedan restaurar.

- Las apps pueden permitir regalar artículos que se pueden comprar dentro de la app a otras personas. Dichos regalos solo se pueden reembolsar al comprador original y no se pueden cambiar.

- Las apps que se distribuyen a través del Mac App Store pueden albergar módulos o extensiones que se habiliten con mecanismos que no sean los del App Store.

- Las apps que ofrecen «cajas de recompensas» u otros mecanismos que proporcionan artículos virtuales aleatorios para la compra deben informar a los clientes de las probabilidades de recibir cada tipo de artículo antes de la compra.

- Las tarjetas regalo digitales, los certificados, los vales y los cupones que se pueden canjear por bienes o servicios digitales solo se pueden vender en tu app mediante compras dentro de la app. Las tarjetas regalo físicas que se venden dentro de una app y luego se envían por correo a los clientes pueden usar métodos de pago diferente a las compras dentro de la app.

- Las apps sin suscripción pueden ofrecer un periodo de prueba gratuito de duración limitada antes de presentar una opción de desbloqueo completo al configurar un artículo de IAP no consumible en el nivel de precio 0 que siga la convención de nomenclatura: «Prueba de XX días». Antes del inicio de la prueba, tu app debe identificar claramente su duración, el contenido o los servicios a los que ya no se podrá acceder cuando finalice la prueba y los cargos posteriores que el usuario

tendría que pagar por la funcionalidad completa. Obtén más información sobre cómo gestionar el acceso al contenido y la duración del periodo de prueba con Recibos y DeviceCheck.

- Las apps pueden usar las compras dentro de la app para vender 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 del NFT no desbloquee prestaciones o funcionalidades dentro de la app. Salvo en la tienda de Estados Unidos, las apps pueden permitir a los usuarios navegar por colecciones de NFT que sean propiedad de terceros, siempre que las apps no incluyan botones, enlaces externos u otras llamadas a la acción que dirijan a los clientes a otros mecanismos de compra diferentes a las compras dentro de la app.

3.1.1 (a) Enlace a otros métodos de compra

Los desarrolladores pueden solicitar autorizaciones para proporcionar en su app un enlace a un sitio web de su propiedad o del que es responsable para la compra de contenidos o servicios digitales. No se requiere que los desarrolladores cuenten con estas autorizaciones para incluir botones, enlaces externos u otras llamadas a la acción en sus apps de la tienda de Estados Unidos. Consulta los detalles adicionales a continuación.

- Autorizaciones de enlace de compra externa de StoreKit: las apps del App Store en regiones específicas pueden ofrecer compras dentro de la app y también usar una autorización de enlace de compra externa de StoreKit para incluir un enlace al sitio web del desarrollador que informa a los usuarios de otras formas de comprar productos o servicios digitales. Obtén más información acerca de estas autorizaciones. De conformidad con los contratos de autorización, el enlace puede informar a los usuarios sobre dónde y cómo deben adquirir esos artículos de compras dentro de la app, y si dichos artículos pueden estar disponibles a un precio comparativamente más bajo. Las autorizaciones solo se pueden usar en el App Store de iOS o iPadOS, en tiendas específicas. En todas las demás tiendas (excepto en la de Estados Unidos, donde esta prohibición no afecta), es posible que las apps y sus metadatos no incluyan botones, enlaces externos u otras llamadas a la acción que dirijan a los clientes a otros mecanismos de compra que no sean compras dentro de la app.

- Autorización de los servicios de música en streaming: las apps de música en streaming de determinadas regiones pueden utilizar estas autorizaciones de los servicios de música en streaming para incluir un enlace (que puede adoptar la forma de un botón de compra) al sitio web del desarrollador que informe a los usuarios de otras formas de comprar contenido o servicios de música digital. Estas autorizaciones también permiten a los desarrolladores de apps de música en streaming invitar a los usuarios a proporcionar su dirección de correo electrónico con el propósito expreso de enviarles un enlace al sitio web del desarrollador para comprar contenido o servicios de música digital. Obtén más información acerca de estas autorizaciones. De conformidad con los contratos de autorización, el enlace puede informar a los usuarios sobre dónde y cómo comprar esos artículos de compras dentro de la app, y el precio de dichos artículos. Las autorizaciones solo se pueden usar en el App Store de iOS o iPadOS, en tiendas específicas. En todas las demás tiendas, es posible que las apps de música en streaming y sus metadatos no incluyan botones, enlaces externos u otras llamadas a la acción que dirijan a los clientes a otros mecanismos de compra que no sean las compras dentro de la app.

- Si tu app tuviera alguna vinculación con prácticas de marketing engañosas, estafas o fraudes que tengan relación con la autorización, será eliminada del App Store. Asimismo, también se te podría expulsar del Apple Developer Program.

3.1.2 Suscripciones

Las apps pueden ofrecer suscripciones de compras dentro de la app con renovación automática, independientemente de la categoría en el App Store. Al incorporar suscripciones que se renuevan automáticamente en la app, asegúrate de seguir las directrices siguientes.

3.1.2 (a) Usos permitidos

Si ofreces una suscripción con renovación automática, debes proporcionar al cliente un valor a largo plazo. Además, el periodo de suscripción debe durar al menos siete días y la app debe estar disponible en todos los dispositivos del usuario. Si bien la lista no es exhaustiva, algunos ejemplos de suscripciones apropiadas son: nuevos niveles de juegos, contenido por episodios, soporte multijugador, apps que ofrecen actualizaciones constantes y sustantivas, acceso a grandes colecciones de contenido multimedia o que se actualizan continuamente, software como servicio («SAAS») y soporte para la nube. Además de lo anterior:

- Las suscripciones se pueden ofrecer junto con una serie de ofertas para elegir (por ejemplo, puedes ofrecer una suscripción a una biblioteca completa de películas, así como para la compra o alquiler de una sola película).

- Los juegos ofrecidos en una suscripción a un servicio de transmisión de juegos pueden ofrecer una única suscripción que se comparte entre apps y servicios de otros fabricantes; sin embargo, deben descargarse directamente del App Store, deben estar diseñadas para evitar el pago duplicado por parte del suscriptor y no deben perjudicar a los clientes no suscriptores.

- Las suscripciones deben funcionar en todos los dispositivos del usuario donde la app esté disponible. Obtén más información sobre cómo compartir una suscripción entre tus apps.

- Como todas las apps, las que ofrecen suscripciones deben permitir a un usuario obtener aquello por lo que ha pagado sin tener que realizar otras tareas, como realizar publicaciones en redes sociales, subir contactos, entrar en la app un número determinado de veces, etc.

- Las suscripciones pueden incluir elementos para consumir como créditos, gemas, divisas que se usan en los juegos, etc., y puedes ofrecer suscripciones que incluyan acceso a bienes de consumo con descuento (por ejemplo, una inscripción de categoría de platino que incluya paquetes de gemas por un precio reducido).

- Si estás cambiando tu app actual a un modelo de negocio basado en suscripciones, no debes eliminar las funciones principales por las que ya han pagado los usuarios. Por ejemplo, permite que los clientes que ya han comprado un «desbloqueo completo de juego» sigan accediendo al juego completo después de introducir un modelo de suscripción para los clientes nuevos.

- Las apps con suscripciones que se renuevan automáticamente pueden ofrecer un periodo de prueba gratuito a los clientes proporcionando la información relevante establecida en App Store Connect. Más información sobre cómo ofrecer ofertas de suscripciones.

- Las apps que intenten estafar a los usuarios se eliminarán del App Store. Esto incluye las apps que intentan engañar a los usuarios para que compren una suscripción bajo falsos pretextos o que se involucren en prácticas engañosas y fraudulentas; estas se eliminarán del App Store y es posible que se eliminen del Apple Developer Program.

- Las apps de telefonía móvil pueden incluir la renovación automática de suscripciones de música y vídeo si se compran en paquetes con planes de datos móviles, con aprobación previa 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 aprobación previa de Apple, si las apps de telefonía móvil permiten las compras dentro de la app para los usuarios. Dichas suscripciones no pueden incluir acceso a artículos consumibles ni descuentos para ellos, y las suscripciones deben finalizar coincidiendo con el plan de datos móviles.

3.1.2 (b) Actualización o retroceso a una versión anterior

Los usuarios deben poder disfrutar de una experiencia de actualización o retroceso a una versión anterior fluida y no debe darse el caso de que se suscriban sin darse cuenta en múltiples variantes de la misma cosa. Revisa las prácticas recomendadas sobre la gestión de las opciones de ampliación y reducción de la suscripción.

3.1.2 (c) Información de suscripción

Antes de pedir a un cliente que se suscriba, deberías describir claramente qué obtendrá por ese precio. ¿Cuántas ediciones al mes? ¿Cuánto almacenamiento en la nube? ¿Qué tipo de acceso a tu servicio? Debes comunicar con claridad los requisitos descritos en el Apéndice 2 del Contrato de Licencia del Apple Developer Program.

3.1.3 Otros métodos de compra

Las siguientes apps pueden usar métodos de compra diferentes a las compras dentro de la app. Las apps de esta sección no pueden, dentro de la app, alentar a los usuarios a usar un método de compra que no sea las compras dentro de la app, excepto para las apps de la tienda de Estados Unidos y tal como se establece en los apartados 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 diferentes a las compras dentro de la app.

3.1.3 (a) Apps de «lector»

Las apps pueden permitir que un usuario acceda a suscripciones o contenido comprado anteriormente (específicamente, revistas, periódicos, libros, audio, música y vídeo). Las apps de lector pueden ofrecer creación de cuentas para niveles gratuitos y una funcionalidad de gestión de cuentas para los clientes existentes. Los desarrolladores de apps de lector pueden solicitar la autorización de la cuenta de enlace externo para proporcionar un enlace informativo en su app a un sitio web del que sea propietario

o responsable para crear o gestionar una cuenta. No se requiere que los desarrolladores cuenten con esta autorización para incluir botones, enlaces externos u otras llamadas a la acción en sus apps de la tienda de Estados Unidos. Obtén más información sobre la autorización de cuentas de 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 prestaciones que hayan adquirido en tu app en otras plataformas o en tu sitio web, incluidos los artículos consumibles en juegos multiplataforma, siempre que esos 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 sus empleados o estudiantes (por ejemplo, bases de datos profesionales y herramientas de gestión del aula), puedes permitir que los usuarios empresariales accedan a contenido o suscripciones que se hayan comprado anteriormente. Las ventas para consumidores, usuarios individuales o familias deben usar las compras 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 (por ejemplo, tutorías, consultas médicas, visitas guiadas del sector inmobiliario o entrenamiento físico), puedes usar métodos de compra diferentes a las compras dentro de la app para cobrar esos pagos. Los servicios en tiempo real personales o de grupo deben usar las compras dentro de la app.

3.1.3 (e) Bienes y servicios fuera de la app

Si la app permite que las personas compren bienes o servicios físicos que se van a consumir fuera de la app, deberás utilizar métodos de compra que no sean las compras dentro de la app para recopilar esos pagos, como Apple Pay o la introducción de tarjetas de crédito tradicionales.

3.1.3 (f) Apps independientes gratuitas

Las apps gratuitas que actúan como complemento independiente de una herramienta web de pago (por ejemplo, VoIP, almacenamiento en la nube, servicios de correo electrónico, alojamiento web) no necesitan usar compras dentro de la app, siempre que no haya compras dentro de la app o llamadas a la acción para comprar fuera de la app.

3.1.3 (g) Apps de gestión de publicidad

Para las apps cuyo único fin es permitir a los anunciantes (personas o empresas que anuncian un producto, servicio o evento) comprar y gestionar campañas publicitarias en distintos tipos de medios (televisión, exteriores, sitios web, apps, etc.), no es necesario usar las compras dentro de la app. Estas apps están destinadas a la gestión de campañas y no muestran anuncios. Las compras digitales de contenido que se experimentan o se consumen en una app, incluida la compra de anuncios para

mostrar en la misma app (como las ventas de «mejoras» para publicaciones en una app de redes sociales) deben usar las compras dentro de la app.

3.1.4 Contenido específico del hardware

En circunstancias muy específicas, como cuando las prestaciones dependen de un hardware concreto para funcionar, la app puede desbloquear esa funcionalidad sin usar las compras dentro de la app (por ejemplo, una app sobre astronomía que añade prestaciones cuando se sincroniza con un telescopio). Las prestaciones de la app que precisan un producto físico aprobado (como un juguete) de forma opcional para funcionar pueden desbloquear prestaciones sin usar las compras dentro de la app, siempre que haya también una opción para este tipo de compras. No obstante, no puedes exigir a los usuarios que compren productos no relacionados o que se impliquen en actividades de publicidad o marketing para desbloquear la funcionalidad de la app.

3.1.5 Criptomonedas

(i) Carteras: las apps pueden facilitar el almacenamiento de moneda virtual, siempre que las ofrezcan desarrolladores inscritos como organización.

(ii) Minería: las apps no pueden utilizar criptomonedas a menos que el procesamiento se realice fuera del dispositivo (por ejemplo, minería basada en la nube).

(iii) Intercambios: las apps pueden facilitar transacciones o transmisiones de criptomonedas en un intercambio aprobado, siempre que se ofrezcan solo en países o regiones donde la app tenga las licencias y los permisos adecuados para proporcionar un intercambio de criptomonedas.

(iv) Ofertas iniciales de monedas: las apps que faciliten las ofertas iniciales de monedas («ICO»), el comercio de futuros de criptomonedas y otras operaciones de criptovalores o cuasivalores deben provenir de bancos establecidos, firmas de inversión, comerciantes de comisiones de futuros («FCM») u otras instituciones financieras aprobadas y deben cumplir todas las leyes aplicables.

(v) Es posible que las apps de criptomonedas no ofrezcan dinero para completar tareas, como descargar otras apps, animar a otros usuarios a descargar, publicar en redes sociales, etc.

3.2 Otros problemas del modelo empresarial

Las listas siguientes no son exhaustivas y el envío puede provocar un cambio o una actualización de nuestras políticas, pero estas son algunas de las cosas que se pueden y no se pueden hacer y que no debes olvidar:

3.2.1 Aceptable

(i) Mostrar tus propias apps para comprar o promocionar dentro de la app, siempre que esta no sea simplemente un catálogo de estas.

(ii) Mostrar o recomendar una colección de apps de otros fabricantes diseñadas para una determinada necesidad aprobada (por ejemplo, gestión sanitaria, aviación, accesibilidad). Tu app debe proporcionar contenidos editoriales sólidos para que no parezca un mero escaparate.

(iii) Deshabilitar el acceso a un determinado contenido de alquiler aprobado (por ejemplo, películas, series, música, libros) una vez que haya expirado el periodo de alquiler. El resto de los artículos y servicios no caducarán.

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

(v) Las apps de seguros deben ser gratuitas, deben cumplir las normativas legales de las regiones donde se distribuyen y no pueden usar las compras dentro de la app.

(vi) Las organizaciones sin ánimo de lucro aprobadas pueden recaudar fondos directamente en sus apps o en las de otros fabricantes, siempre que las campañas de recaudación de fondos se adhieran a todas las Directrices de App Review y sean compatibles con Apple Pay. Estas apps deben incluir información sobre el uso que se hará de los fondos, cumplir todas las leyes locales y federales pertinentes, y garantizar que todas las personas donantes tienen a su disposición los recibos fiscales correspondientes. Se proporcionará información adicional a App Review si se solicita. Las plataformas sin ánimo de lucro que conectan a donantes con otras organizaciones sin ánimo de lucro deben asegurarse de que todas ellas han superado el proceso de aprobación de este tipo de organizaciones. Obtén más información sobre cómo convertirse en una organización sin ánimo de lucro aprobada.

(vii) Las apps pueden permitir a los usuarios hacer regalos monetarios a otra persona sin usar las compras de la app, siempre que (a) el regalo sea una elección totalmente opcional del dador y que (b) el 100 % de los fondos vayan al destinatario del regalo. No obstante, los regalos que en algún momento estén relacionados o asociados con la recepción de contenido o servicios digitales deben usar las compras dentro de la app.

(viii) Las apps que se utilizan para operaciones financieras, inversiones o gestión de fondos deben enviarlas la institución financiera que realiza dichos servicios y deben tener las licencias y permisos necesarios en las ubicaciones donde las pones a disposición.

3.2.2 Inaceptable

(i) Crear una interfaz para mostrar apps, extensiones o módulos de otros fabricantes similares al App Store o como una colección de interés general.

(ii) Omisión intencionada.

(iii) Aumentar de forma artificial el número de impresiones o clics que reciben los anuncios, así como las apps que se han diseñado predominantemente para mostrar anuncios.

(iv) A menos que seas una organización sin ánimo de lucro aprobada o que lo estipulado en la sección 3.2.1 (vi) anterior lo permita, recaudar fondos dentro de la app para organizaciones benéficas y campañas de recaudación de fondos. Las apps cuya finalidad es conseguir dinero para estas causas deben ser gratuitas en el App Store y solo pueden recaudar fondos fuera de la app; por ejemplo, a través de Safari o mensajes SMS.

(v) Restringir de forma arbitraria quién puede usar la app en función de la ubicación o el operador, por ejemplo.

(vi) Omisión intencionada.

(vii) Manipular artificialmente la visibilidad, el estado o la clasificación del usuario en otro servicio, a menos que lo permitan los términos y condiciones de dicho servicio.

(viii) En el App Store no se admiten apps que faciliten las operaciones bursátiles con opciones de retorno fijo. Es preferible recurrir a una app web. Las apps que facilitan la operación con contratos por diferencia («CFD») u otros derivados (por ejemplo, FOREX) deben tener la licencia correspondiente en todas las jurisdicciones donde el servicio esté disponible.

(ix) Las apps que ofrecen préstamos personales deben revelar 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 préstamo no pueden cobrar una APR máxima superior al 36 %, incluidos costes y cargos, y no pueden requerir el reembolso total en 60 días o menos.

(x) Las apps no deben forzar a los usuarios a realizar valoraciones o revisiones sobre ellas, descargar otras apps u otras acciones relacionadas con la tienda para poder acceder a sus funciones, a su contenido o para hacer uso de ellas. Las apps sí pueden incentivar 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 especialmente los productos que son sencillos, precisos, innovadores y fáciles de usar, y eso es lo que quieren ver en el App Store. Presentar un diseño fantástico es algo que tú debes decidir, pero estos son estándares mínimos de aprobación del App Store. Recuerda que, incluso después de que se haya aprobado la app, debes actualizarla para asegurarte de que sigue estando operativa y de que todavía atrae a clientes nuevos y existentes. Las apps que dejen de funcionar o que ofrezcan una experiencia deteriorada se pueden eliminar del App Store en cualquier momento.

4.1 Imitaciones

(a) Presenta tus propias ideas. Sabemos que las tienes, así que plásmalas y muéstralas. No te limites a copiar la última app popular del App Store ni a hacer pequeños cambios en el nombre o la interfaz de usuario de otra app para presentarla como propia. Además de que esto podría infringir los derechos de propiedad intelectual y dificultar el desplazamiento por el App Store, no es justo para el resto de los desarrolladores.

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

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

4.2 Funcionalidad mínima

La app debe incluir prestaciones, contenido y opciones de la interfaz de usuario que la eleven a algo más que un sitio web de paquetes. Si tu app no es particularmente útil, exclusiva o «similar a una app», no es para el App Store. Es posible que la app no se acepte si no proporciona algún tipo de valor duradero de entretenimiento o de utilidad adecuada. Las apps que sean simplemente una canción o una película deben enviarse al iTunes Store. Las apps que están formadas por una guía de libros o juegos se deben enviar al Apple Books Store.

4.2.1 Las apps que usen ARKit deben integrar experiencias de realidad aumentada completas; no basta con mostrar un modelo en una vista de realidad aumentada o con reproducir una animación.

4.2.2 Excepto los catálogos, las apps no deben ser primordialmente materiales de marketing, anuncios, recortes web, agregadores de contenido ni colecciones de enlaces.

4.2.3

(i) La app debe funcionar por sí misma, sin necesitar la instalación de otra app para ello.

(ii) Si tu app necesita descargar recursos adicionales para funcionar en el lanzamiento inicial, indica el tamaño de la descarga y pregunta a los usuarios antes de hacerlo.

4.2.4 Omisión intencionada.

4.2.5 Omisión intencionada.

4.2.6 Las apps que se hayan creado con una plantilla comercial o un servicio de generación de apps se rechazarán, a menos que el proveedor del contenido de la app los 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 proporcionen experiencias únicas. Otra opción aceptable para los proveedores de plantillas es crear un único binario para alojar todo el contenido del cliente en un modelo agregado o de selección, por ejemplo, como una app de búsqueda de restaurantes con entradas o páginas personalizadas independientes para cada restaurante del cliente, o como una app de eventos con entradas separadas para cada evento del cliente.

4.2.7 Clientes de escritorio remoto

Si tu app de escritorio remoto actúa como un espejo de software o servicios específicos en lugar de como un espejo genérico del dispositivo host, debe cumplir lo siguiente:

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

(b) Cualquier software o servicio que aparezca en el cliente se ejecuta por completo en el dispositivo host, se muestra en la pantalla del dispositivo host y no puede usar API o prestaciones de la plataforma más allá de lo que se requiere para transmitir el Escritorio remoto.

(c) Toda la creación y gestión de cuentas debe iniciarse desde el dispositivo host.

(d) La interfaz de usuario que aparece en el cliente no se parece a una vista de iOS o App Store, no proporciona una interfaz de tipo tienda, ni incluye la capacidad de navegar, seleccionar ni comprar software que aún no sea propiedad del usuario o que no tenga licencia. A título aclaratorio, las transacciones que se realizan dentro del software duplicado no necesitan usar las compras dentro de la app, siempre que las transacciones se procesen en el dispositivo host.

(e) Para el App Store, no son adecuados los clientes ligeros para apps basadas en la nube.

4.3 Spam

(a) No crees varios identificadores de paquete de la misma app. Si la app tiene diferentes versiones para determinadas ubicaciones, equipos deportivos, universidades, etc., considera la opción de enviar una única app y proporcionar las variantes con la opción de compras dentro de la app.

(b) Asimismo, evita forzar su inclusión en una categoría que ya esté saturada; el App Store ya tiene suficientes apps de pedos, eructos, linternas, adivinación del futuro, citas, juegos de beber y Kama Sutra. Rechazaremos estas apps a menos que ofrezcan una experiencia única y de alta calidad. Enviar correos no deseados a la tienda puede provocar tu eliminación del 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 algunas funciones, como pantallas de ayuda e interfaces de configuración, siempre que sea posible. Debes indicar de forma clara y precisa qué extensiones están disponibles en el texto de marketing de la app; las extensiones no pueden incluir marketing, anuncios ni compras dentro de la app.

4.4.1 Las extensiones de teclado tienen algunas reglas adicionales.

Deben cumplir lo siguiente:

- proporcionar funcionalidad de entrada de teclado (por ejemplo, caracteres escritos);
- cumplir las directrices para stickers, si el teclado incluye imágenes o emojis;
- proporcionar un método para pasar al siguiente teclado;
- seguir operativas sin acceso completo a la red y sin requerir acceso total;
- recoger la actividad del usuario únicamente para mejorar la funcionalidad de la extensión de teclado del usuario en el dispositivo iOS.

No deben:

- iniciar otras apps además de Ajustes; ni
- destinar a otros comportamientos los botones del teclado (por ejemplo, mantener presionada la tecla Intro para iniciar 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 pueden interferir con los elementos del sistema o la interfaz de usuario de Safari y nunca deben incluir código o contenido engañoso o creado con fines malintencionados. Si se infringe esta norma, se eliminará del Apple Developer Program. Las extensiones de Safari no deben poder acceder a más sitios web que los estrictamente necesarios para la función.

4.4.3 Omisión intencionada.

4.5 Sitios y servicios de Apple

4.5.1 Las apps pueden usar canales RSS de Apple aprobados, como el canal RSS de iTunes Store, pero no pueden extraer información de los sitios de Apple (por ejemplo, apple.com, iTunes Store, App Store, App Store Connect, portal de 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 local de forma nativa desde tus apps y juegos. Cuando un usuario da permiso a su cuenta de Apple Music, tu app puede crear listas de reproducción, añadir canciones a su biblioteca y reproducir cualquiera de los millones de canciones del catálogo de Apple Music. Los usuarios deben empezar a reproducir una secuencia de Apple Music y tener acceso a los controles multimedia estándar, como «reproducir», «pausar» y «saltar». Además, la app no puede exigir el pago del servicio de Apple Music ni monetizar indirectamente el acceso a este (por ejemplo, mediante compras dentro de la app, publicidad o la solicitud de información del usuario). No cargues ni descargues archivos de música

procedentes de las API de MusicKit, ni permitas que se compartan, a menos que la documentación de MusicKit lo permita expresamente.

(ii) Las API de MusicKit no son un sustituto para asegurarte las licencias que puedas necesitar para una integración mayor o más compleja. Por ejemplo, si quieres que tu app reproduzca una canción específica en un momento determinado o que cree archivos de audio o vídeo que se puedan compartir en las redes sociales, debes ponerte en contacto directamente con los titulares de los derechos para obtener su permiso (por ejemplo, derechos de sincronización o adaptación) y sus materiales. Las portadas de discos y otros metadatos solo se pueden usar cuando van asociados a la reproducción de música o a listas de reproducción (por ejemplo, en capturas de pantalla del donde se muestre el funcionamiento de la app). No se deben usar en contenido de marketing o publicitario sin la autorización expresa de los titulares de los derechos. Asegúrate de seguir las indicaciones de las Directrices de identidad de Apple Music al integrar los servicios de Apple Music en tu app.

(iii) Las apps que accedan a datos de los usuarios de Apple Music, como listas de reproducción y favoritos, deben mencionar dicho acceso claramente en el apartado donde se describa su uso. Los datos recopilados no se pueden compartir con terceros para ningún fin, salvo para facilitar o mejorar la experiencia con la app. Estos datos no se pueden usar para identificar a usuarios o dispositivos, ni para segmentar la publicidad.

4.5.3 No utilices los servicios de Apple para enviar mensajes no deseados, realizar actividades de phishing o enviar mensajes no solicitados a los clientes, incluidos el Game Center, las notificaciones push, etc. No intentes hacer búsquedas inversas, rastrear, relacionar, asociar, extraer, recopilar o explotar de alguna otra forma los identificadores y los alias del reproductor, o cualquier otra información que se obtenga a través del Game Center. De lo contrario, se te eliminará del Apple Developer Program.

4.5.4 Para que la app funcione no se deben exigir las notificaciones push y no se deben usar para enviar información confidencial o personal sensible. Las notificaciones push no deben usarse para promociones o con fines de marketing directo, a menos que los clientes hayan optado explícitamente por recibirlas a través del texto de consentimiento que se muestra en la interfaz de usuario de tu app, y tú proporcionarás un método en tu app para que el usuario opte por no recibir dichos mensajes. El mal uso de estos servicios puede provocar revocación de tus privilegios.

4.5.5 Utiliza solo los identificadores del reproductor de Game Center de una manera que esté aprobada por las condiciones del Game Center y no los muestres en la app o a otro fabricante.

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

4.6 Omisión intencionada.

4.7 Miniapps, minijuegos, juegos en streaming, chatbots, módulos y emuladores de juegos

Las apps pueden ofrecer determinado software que no esté integrado en el binario, específicamente miniapps, minijuegos en HTML5 y JavaScript, juegos en streaming, chatbots y módulos. Además, las apps de emulador de videoconsolas y PC retro ofrecen la posibilidad de descargar juegos. Tú eres responsable de todo el software ofrecido en tu app, lo que incluye asegurarte de que dicho software cumpla las presentes directrices y todas las leyes aplicables. El incumplimiento de cualquier directriz en este software provocará el rechazo de tu app. También debes asegurarte de que el software cumple las normas adicionales que se indican en los apartados del 4.7.1 al 4.7.5. Estas normas adicionales son importantes para preservar la experiencia que esperan los clientes del App Store y para ayudar a garantizar la seguridad del usuario.

4.7.1 El software ofrecido en las apps bajo esta regla debe:

- seguir todas las directrices de privacidad, incluidas, entre otras, las reglas establecidas en la Directriz 5.1 respecto a la recopilación, uso y uso compartido de datos y datos confidenciales (por ejemplo, datos de salud o datos personales de niños);
- incluir un método para filtrar el material censurable, un mecanismo para denunciar el contenido ofensivo y ofrecer una respuesta rápida a los problemas, y la capacidad de bloquear a los usuarios abusivos; y
- siga la Directriz 3.1 para utilizar las compras dentro de la app y ofrecer bienes o servicios digitales a los usuarios finales.

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

4.7.3 Tu app no puede compartir datos ni permisos de privacidad con ningún software ofrecido 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. Debe incluir enlaces universales que conduzcan a todo el software que se ofrece en tu app.

4.7.5 Tu app debe ofrecer a los usuarios una forma de identificar el software que supere la clasificación por edades de la app y utilizar un mecanismo de restricción por 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 utilizan un servicio de inicio de sesión social o de otros fabricantes (como inicio de sesión de Facebook, inicio de sesión de 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 prestaciones:

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

La cuenta principal de un usuario es la cuenta que establece con tu app para identificarse, iniciar sesión y acceder a tus prestaciones y servicios asociados.

No se requiere otro servicio de inicio de sesión si:

- Tu app utiliza exclusivamente los sistemas de inicio de sesión y 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 utiliza un inicio de sesión específico de dicho mercado para las prestaciones de cuenta, descarga y comercio.
- Tu app es una app educativa o empresarial que requiere que el usuario inicie sesión con una cuenta educativa o empresarial existente.
- Tu app utiliza un sistema de identificación de ciudadanos o un documento de identidad electrónico respaldado por el gobierno o la industria para autenticar a los usuarios.
- Tu app es un cliente de un servicio de otros fabricantes 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 utilizan Apple Pay deben proporcionar al usuario toda la información relacionada con la compra del material antes de vender cualquier bien o servicio, y deben usar la marca de Apple Pay y los elementos de la interfaz de usuario correctamente, como se describe en las Directrices de marketing de Apple Pay y en las Directrices de interfaz humana. Las apps que utilizan 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 hasta que se cancele.
- Qué se proporcionará durante cada periodo.
- Los cargos reales que se facturarán al cliente.
- Cómo cancelar.

4.10 Monetizar las capacidades integradas

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

---

5. Aspectos legales

Las apps deben cumplir todos los requisitos legales del lugar en el que estén disponibles (si no estás seguro, comprueba estos aspectos con un abogado). Sabemos que esto es complicado, pero es tu responsabilidad comprender y asegurarte de que tu app cumple con todas las leyes locales, no solo con las directrices que se indican a continuación. Y, por supuesto, se rechazarán las apps que solicitan, promueven o fomentan comportamientos criminales o claramente temerarios. En casos extremos, por ejemplo, si se demuestra que las apps facilitan el tráfico de personas o la explotación infantil, se informará a las autoridades competentes.

5.1 Privacidad

Proteger la privacidad del usuario es primordial en el ecosistema Apple y debes prestar una especial atención cuando manipules datos personales para garantizar que cumples con las prácticas recomendadas de privacidad, las leyes aplicables y las condiciones del Contrato de Licencia del Apple Developer Program, por no mencionar las expectativas de los clientes. Más concretamente:

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, de forma clara y precisa, debe:

- Identificar qué datos, si los hay, recopila la app/servicio, cómo recopila esos datos y todos los usos que se dan a esos datos.
- Confirmar que cualquier tercero con el que una app comparta datos de usuario (de acuerdo con estas Directrices), como herramientas de análisis, redes de publicidad y SDK de otros fabricantes, así como cualquier entidad matriz, subsidiaria u otra entidad relacionada que tenga acceso a los datos del usuario: proporcionará la misma protección de los datos del usuario que se establece en la política de privacidad de la app y que se exige en estas Directrices.
- Explicar sus políticas de retención/eliminación de datos y describir cómo un usuario puede revocar el consentimiento y/o solicitar la eliminación de los datos del usuario.

(ii) Permiso: las apps que recopilan datos de usuario o de 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 depender de ni exigir que un usuario otorgue acceso a estos datos. Las apps también deben proporcionar al cliente una forma comprensible y de fácil acceso para retirar el consentimiento. Asegúrate de que el texto sobre el propósito de la app describe de forma clara y completa el uso que haces de los datos. Las apps que recopilan datos para un interés legítimo sin consentimiento mediante los términos del Reglamento General de Protección de Datos («RGPD») o un estatuto similar deben cumplir 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 la funcionalidad principal de la app y solo deben recopilar y usar los datos necesarios para realizar la tarea correspondiente. Siempre que sea posible, usa el selector fuera de proceso o una hoja para compartir en lugar de solicitar acceso completo 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 obligar 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 que el usuario cargue fotos. Siempre que sea posible, ofrece soluciones alternativas a los usuarios que no otorgan su consentimiento. Por ejemplo, si un usuario se niega a compartir la ubicación, ofrece la posibilidad de introducir una dirección manualmente.

(v) Inicio de sesión en la cuenta: si tu app no incluye prestaciones importantes basadas en la cuenta, permite que la gente la use 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 deben precisar que se introduzca información personal para usarlas a menos que sea relevante de forma directa para su funcionalidad principal o así lo exija la ley. Si la funcionalidad principal de tu app no está relacionada con una red social específica (por ejemplo, Facebook, WeChat, Weibo, X, etc.), debes proporcionar acceso sin iniciar sesión o mediante otro mecanismo. Extraer información básica del perfil, compartirla en la red social o invitar a amigos a usar la app no se consideran funciones básicas de la app. La app también debe incluir un mecanismo para revocar las credenciales de la red social y desactivar el acceso a los datos entre la app y la red social desde dentro de la app. Una app no puede almacenar credenciales o tokens en redes sociales fuera del dispositivo y solo puede usar dichas credenciales o tokens para conectarse directamente a la red social desde la propia app mientras esta esté en uso.

(vi) Los desarrolladores que utilizan sus apps para descubrir de forma oculta las contraseñas u otros datos privados se eliminarán del Apple Developer Program.

(vii) Se debe utilizar SafariViewController para presentar de forma visible información a los usuarios; el controlador no debe quedar oculto por otras vistas o capas. Además, una app no puede usar SafariViewController para rastrear 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 las bases de datos públicas, no están permitidas en el App Store ni en métodos de distribución alternativos.

(ix) Las apps que prestan servicios en ámbitos muy regulados (como servicios bancarios y financieros, atención sanitaria, juegos de azar, consumo legal de cannabis, viajes en avión e intercambios de criptomonedas) o que requieren información confidencial del usuario deben ser enviadas por una entidad legal que proporcione los servicios y 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 que la solicitud sea opcional para el usuario, las prestaciones y los servicios no estén condicionados a proporcionar la información y cumplan con todas las demás disposiciones de estas directrices, incluidas las limitaciones a la hora 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 otra persona sin antes obtener su permiso. Debes proporcionar acceso a información sobre cómo y dónde se utilizarán los datos. Debes indicar claramente dónde se compartirán los datos personales con terceros, incluida la IA de otros fabricantes, y obtener un permiso explícito antes de hacerlo. Los datos recopilados de las apps solo pueden compartirse con terceros para mejorar la app o distribuir publicidad (de conformidad con el Contrato de Licencia del Apple Developer Program). Debes recibir permiso explícito de los usuarios a través de las API de transparencia en el seguimiento de las apps para rastrear su actividad. Obtén más información sobre el seguimiento. Puede que tu app no requiera que los usuarios activen funcionalidades del sistema (por ejemplo, las notificaciones push, los servicios de ubicación o el seguimiento) para acceder a la funcionalidad o el contenido, usar la app o recibir una compensación monetaria o de otro tipo, lo que incluye, entre otras cosas, tarjetas regalo y códigos. Las apps que comparten datos del usuario sin su consentimiento o que cumplen con las leyes de privacidad de datos pueden quedar fuera de la venta y pueden dar lugar a su eliminación del Apple Developer Program.

(ii) Los datos recopilados para un propósito no pueden reutilizarse sin consentimiento, a menos que la ley lo permita explícitamente.

(iii) Las apps no deben intentar crear de forma encubierta un perfil de usuario basado en los datos recopilados ni deben intentar, permitir ni incitar a otros a identificar a usuarios anónimos o reconstruir perfiles de usuario a partir de los datos recopilados por las API proporcionadas por Apple o los datos que afirmas que se han recopilado de forma «anónima», «colectiva» o que impide la identificación.

(iv) No utilices 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/distribución a terceros, y no recopiles información sobre qué otras apps están instaladas en el dispositivo de un usuario con fines de análisis o publicidad/marketing.

(v) No se ponga en contacto con personas que utilicen la información recopilada a través de los contactos o las fotos de un usuario, excepto por iniciativa explícita de ese usuario de forma individualizada; no incluyas la opción Seleccionar todo o la selección predeterminada de todos

los contactos. Debes proporcionar al usuario una descripción clara de cómo se verá el mensaje al destinatario antes de enviarlo (por ejemplo, ¿qué dirá el mensaje?, ¿quién aparecerá como remitente?).

(vi) Los datos recopilados desde la API HomeKit, HealthKit, la API Clinical Health Records, las API MovementDisorder, ClassKit o herramientas de detección de profundidad o mapeo facial (como ARKit o las API de cámara o de fotos) no se pueden utilizar con fines publicitarios o de minería de datos basada en el uso, ni siquiera por parte de terceros. 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 datos de usuario adquiridos a través de Apple Pay con otros fabricantes para facilitar o mejorar la entrega de bienes y servicios.

5.1.3 Salud e investigación sanitaria

Los datos de salud, fitness y médicos son especialmente confidenciales y las apps de este espacio tienen algunas reglas adicionales para garantizar la protección de la privacidad del cliente:

(i) Las apps no pueden usar o revelar a terceros datos recopilados en el contexto de la salud, el fitness o estudios médicos (incluidos aquellos extraídos de la API Clinical Health Records, la API HealthKit, las API Motion y Fitness, y MovementDisorder, o de investigaciones relacionadas con seres humanos) para publicidad, marketing u otros fines de recopilación de datos basada en los usuarios que no sean los de mejorar la gestión sanitaria o para realizar investigaciones en salud y, en ese caso, solo con permiso. Sin embargo, las apps pueden usar los datos de salud o fitness de un usuario para proporcionar un beneficio directamente a ese usuario (como una prima de seguro reducida), siempre que la app sea enviada por la entidad que proporciona el beneficio y los datos no se compartan con un tercero. Debes revelar los datos de salud específicos que estás recopilando del dispositivo.

(ii) Las apps no deben escribir datos falsos o imprecisos en HealthKit ni en otra app de gestión sanitaria o investigación médica. Tampoco pueden almacenar información sanitaria personal en iCloud.

(iii) Las apps que realizan investigaciones con seres humanos 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, riesgos y beneficios para el participante; (c) la información sobre la confidencialidad y el tratamiento de los datos (incluido el intercambio con terceros); (d) un punto de contacto para las preguntas de los participantes; y (e) el proceso de retirada.

(iv) Las apps que lleven a cabo investigaciones en seres humanos deben contar con la aprobación de un comité de ética independiente. Se debe proporcionar una prueba de dicha aprobación previa solicitud.

5.1.4 Niños

(a) Por muchos motivos, es fundamental manejar con extremo cuidado los datos personales de los niños. Te animamos a que revises detenidamente todos los requisitos para cumplir la legislación al respecto, como la Ley de Protección de la Privacidad Infantil en Internet de Estados Unidos (Children's Online Privacy Protection Act, «COPPA»), el Reglamento General de Protección de Datos («RGPD») de la Unión Europea y otras leyes o normativas aplicables.

Las apps pueden solicitar la fecha de nacimiento e información de contacto parental solo para cumplir estos estatutos, pero deben incluir alguna funcionalidad útil o un valor de entretenimiento independientemente de la edad de la persona.

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

(b) En casos limitados, los análisis de otros fabricantes y la publicidad de otros fabricantes pueden estar permitidos siempre que los servicios se adhieran a los mismos términos establecidos en la Directriz 1.3.

Además, las apps de la categoría de niños o aquellas que recopilan, transmiten, o tienen la capacidad de compartir información personal (como el nombre, la dirección postal, la dirección de correo electrónico, la ubicación, las fotos, los vídeos, los dibujos, la capacidad para chatear, otros datos personales o identificadores persistentes que se utilizan junto con alguno de los elementos anteriores) de un menor deben incluir una política de privacidad y deben cumplir todos los estatutos de privacidad para niños que apliquen. Para mayor claridad, el requisito de acceso para padres en la categoría de niños no es, generalmente, lo mismo que garantizar el consentimiento paterno para recopilar datos personales según estas leyes sobre privacidad.

Como recordatorio, la Directriz 2.3.8 requiere que el uso de términos como «Para niños» y «Para menores» en los metadatos de la app esté reservado a la categoría de niños. Las apps que no están en la categoría de niños no pueden incluir términos en el nombre, el subtítulo, el icono, las capturas de pantalla o la descripción de la app que impliquen que el público objetivo principal de la app son los niños.

5.1.5 Servicios de localización

Usa servicios de localización en tu app solo cuando sea directamente relevante para las prestaciones y servicios que ofrece la app. No se deben utilizar las API basadas en la ubicación para proporcionar servicios de emergencia o el control autónomo sobre vehículos, aviones y otros dispositivos, a excepción de los pequeños dispositivos como juguetes y drones ligeros, o sistemas remotos de alarma para vehículos, etc. Asegúrate de notificar y obtener consentimiento antes de recopilar, transmitir o usar datos de ubicación. Si tu app usa servicios de localización, asegúrate de explicar el propósito en ella; consulta las Directrices de interfaz humana para conocer las prácticas recomendadas.

5.2 Propiedad intelectual

Asegúrate de que la app solo incluya contenido que tú hayas creado o que tengas licencia para usar. Se podría eliminar la app si te extralimitas y utilizas contenido sin permiso. Por supuesto, esto también significa que la app de otra persona se puede borrar también si han tomado prestado contenido de tu trabajo. Si crees que otro desarrollador ha infringido tus derechos de propiedad intelectual en el App Store, envía una reclamación a través de nuestro formulario web. Las leyes difieren en los distintos países y regiones, pero como mínimo, asegúrate de evitar los siguientes errores comunes:

5.2.1 De forma general: no utilices material protegido de otros fabricantes (como pueden ser marcas comerciales, trabajos con derechos de autor o ideas patentadas) en la app si no tienes permiso para hacerlo y no incluyas en el paquete de la app o el nombre del desarrollador representaciones, nombres o metadatos engañosos, falsos o de imitadores. Las apps deben ser enviadas por la persona o entidad jurídica que posee o tiene licencia de la propiedad intelectual y otros derechos relevantes.

5.2.2 Sitios/servicios de otros fabricantes: si tu app usa, accede, monetiza el acceso o muestra contenido de un servicio de otros fabricantes, asegúrate de que tienes permiso para hacerlo según las condiciones de uso del servicio. Se debe proporcionar autorización previa solicitud.

5.2.3 Descarga de audio/vídeo: las apps no deben facilitar el intercambio ilegal de archivos ni incluir la capacidad de guardar, convertir o descargar contenido multimedia de otros fabricantes (por ejemplo, Apple Music, YouTube, SoundCloud, Vimeo, etc.) sin la autorización explícita de dichas fuentes. La transmisión de contenido de audio/vídeo también puede infringir las Condiciones de uso, así que asegúrate de comprobarlo antes de que tu app acceda a esos servicios. Se debe proporcionar autorización previa solicitud.

5.2.4 Aprobaciones de Apple:

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

(b) Si tu app se selecciona como «opción del editor», Apple aplicará el distintivo automáticamente.

5.2.5 Productos Apple: no crees una app que sea tan similar a un producto existente, una interfaz (por ejemplo, Finder), una app (como App Store, iTunes Store o Mensajes) o un tema de publicidad de Apple que se pueda confundir con ellos. Es posible que las apps y extensiones, incluidos los teclados de otros fabricantes y los paquetes de stickers, no incluyan el emoji de Apple. La música de iTunes y las vistas previas de Apple Music no se pueden usar por su valor de entretenimiento (por ejemplo, como música de fondo para un collage de fotos o la banda sonora de un juego) ni de ninguna otra manera no autorizada. Si proporcionas vistas previas de música de iTunes o Apple Music, debes mostrar un enlace a la música correspondiente en iTunes o Apple Music. Si tu app muestra anillos de Actividad, no deben mostrar datos de Movimiento, Ejercicio o De Pie de un modo que se asemeje al control de Actividad. Las Directrices de interfaz humana incluyen más información sobre cómo usar los anillos de Actividad. Si tu app muestra datos meteorológicos de Apple, debe seguir los requisitos de atribución indicados en la documentación de WeatherKit.

5.3 Juegos, apuestas y loterías

Las apuestas, los juegos y las loterías pueden ser bastante delicados a la hora de gestionarlos y tienden a ser una de las ofertas más reguladas del App Store. Incluye únicamente esta funcionalidad si conoces muy bien las obligaciones legales que tendrás en todos los lugares en los que la app vaya a estar disponible y si estás preparado para dedicar tiempo extra al proceso de revisión. Algunos aspectos que se deben tener en cuenta:

5.3.1 Los sorteos y 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 claro que Apple no patrocina ni participa en la actividad de ninguna manera.

5.3.3 Las apps no pueden usar las compras dentro de la app para adquirir crédito o divisa que se vaya a usar en combinación con juegos con dinero real de cualquier tipo.

5.3.4 Las apps que ofrecen juegos con dinero real (por ejemplo, apuestas deportivas, póquer, juegos de casino y carreras de caballos) o loterías deben contar con las licencias y los permisos que se precisen en cada lugar donde se utilice la app, deben estar restringidas geográficamente a esos lugares y deben ser gratuitas en el App Store. Las ayudas ilegales en juegos, incluidos los contadores de cartas, no están permitidas en el App Store. Las apps de lotería deben incluir contraprestación, probabilidad y un premio.

5.4 Apps con red privada virtual (VPN)

Las apps que ofrecen servicios VPN deben utilizar la API de NEVPNManager y solo los pueden ofrecer desarrolladores inscritos como organización. Debes hacer una descripción clara de qué datos del usuario se recopilarán y cómo se usarán en la pantalla de una app antes de que el usuario realice cualquier acción para comprar o usar el servicio. Las apps que ofrecen servicios VPN no pueden vender, usar ni divulgar a terceros ningún dato para ningún fin, y deben cumplir esto en su política de privacidad. Las apps de VPN no deben infringir las leyes locales y, si decides que tu app de VPN esté disponible en un territorio que requiera una licencia de VPN, debes proporcionar la información de tu licencia en el campo Notas para 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 esta directriz se eliminarán del App Store. También se bloqueará su instalación mediante métodos de distribución alternativos y es posible que se te elimine del Apple Developer Program.

5.5 Gestión de dispositivos móviles

Las apps de gestión de dispositivos móviles que ofrecen servicios de gestión de dispositivos móviles (MDM) deben solicitar esta prestación 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 servicios de control parental o seguridad de dispositivos. Debes hacer una descripción clara de qué datos del usuario se recopilarán y cómo se usarán en la pantalla de una app antes de que el usuario realice cualquier acción para comprar o usar el servicio. Las apps de MDM no deben infringir ninguna ley aplicable. Las apps que ofrecen servicios MDM no pueden vender, usar ni divulgar a terceros ningún dato para ningún fin, y deben cumplir esto 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, el dispositivo del usuario u otras apps utilizadas en ese dispositivo. Las apps que ofrecen perfiles de configuración también deben cumplir estos requisitos. Las apps que no cumplan con esta directriz se eliminarán del App Store. También se bloqueará su instalación mediante métodos de distribución alternativos y es posible que se te elimine del 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 cometas ningún tipo de acoso, prácticas discriminatorias, intimidación u hostigamiento, y no animes a otros a participar en ninguna de las situaciones anteriores. Un comportamiento repetido de manipulación o engaño u otra conducta fraudulenta dará lugar a tu eliminación del Apple Developer Program.

La confianza del cliente es una piedra angular del ecosistema de apps. Las apps nunca deben aprovecharse de los usuarios ni intentar estafar a los clientes, engañarlos para que hagan compras no deseadas, obligarlos a compartir datos innecesarios, subir los precios de manera engañosa, cobrar por prestaciones o contenido que no se entregan, ni participar en cualquier otra práctica de manipulación dentro o fuera de la app.

Tu cuenta del Developer Program se cancelará si participas en actividades o acciones que no se ajusten al código de conducta para desarrolladores. Para restaurar tu cuenta, puedes proporcionar una declaración por escrito que detalle las mejoras que planeas hacer. Si Apple aprueba tu plan y confirmamos que se han realizado los cambios, es posible que se restablezca 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 a sus comentarios. Mantén tus respuestas orientadas a los comentarios del usuario y no incluyas información personal, spam o marketing en tu respuesta.

Utiliza la API que se proporciona para solicitar a los usuarios que valoren tu app. Esta funcionalidad permite a los clientes escribir una reseña y valorar tu app en el App Store desde la misma app. No aceptaremos las solicitudes de reseñas personalizadas.

5.6.2 Identidad del desarrollador

Proporcionar información verificable a Apple y a los clientes es fundamental para obtener su confianza. La representación de ti mismo, tu empresa y tus ofertas en el App Store o en métodos de distribución alternativos debe ser precisa. La información que proporciones debe ser veraz, relevante y actualizada para que Apple y los clientes entiendan con quién están interactuando y puedan contactar contigo en relación con cualquier problema.

5.6.3 Fraude de descubrimiento

Participar en el App Store requiere integridad y el compromiso de generar y mantener la confianza de los clientes. Manipular cualquier elemento de la experiencia del cliente del App Store, como gráficos, búsquedas, reseñas o referencias a tu app, afecta a la confianza del cliente y no está permitido.

5.6.4 Calidad de la app

Los clientes esperan la máxima calidad del App Store, y mantener contenidos, servicios y experiencias de alta calidad fomenta la confianza del cliente. Los indicios de que esta expectativa no se está cumpliendo incluyen un número excesivo de informes de clientes sobre problemas con tu app, como reseñas negativas de clientes y un número excesivo de solicitudes de reembolso. La incapacidad de mantener una alta calidad puede ser un factor a la hora de 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 en App Store Connect y estés en el proceso de revisión, debes tener en cuenta los siguientes aspectos:

- **Plazos:** 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. Y recuerda que si tu app es rechazada repetidamente por la misma infracción de las directrices, o si intentas manipular el proceso de revisión de App Review, la revisión de tu app tardará más en completarse. Obtén más información sobre App Review.

- **Actualizaciones de estado:** el estado actual de tu app se reflejará en App Store Connect, para que puedas estar al tanto de todo.

- **Acelerar solicitudes:** si tienes un plazo crítico, puedes solicitar una revisión urgente. Respeta a los demás desarrolladores y únicamente solicita una revisión urgente cuando realmente lo necesites. Si nos percatamos de que estás abusando de este sistema, podríamos rechazar las solicitudes que realices en el futuro.

- **Fecha de publicación:** si tu fecha de publicación se establece para más adelante, la app no aparecerá en el App Store hasta esa fecha, incluso si App Review la ha aprobado. Y recuerda que tu app puede tardar hasta 24 horas en aparecer en todas las tiendas seleccionadas.

- **Rechazos:** nuestro objetivo es aplicar estas directrices de forma justa y coherente, pero nadie es perfecto. Si se ha rechazado tu app y tienes preguntas al respecto, o si quieres proporcionar información adicional, utiliza App Store Connect para ponerte en contacto directamente con el equipo de App Review. De este modo puedes, por una parte, lograr que tu app llegue a la tienda y, por otra, puedes ayudarnos a mejorar el proceso de App Review o identificar algo que se tenga que aclarar en nuestras políticas.

- **Apelaciones:** si no estás de acuerdo con el resultado de tu revisión, envía una apelación. De este modo, puedes lograr que tu app llegue a la tienda. También puedes sugerir cambios en las propias directrices para ayudarnos a mejorar el proceso de App Review o identificar algo que se tenga que aclarar en nuestras políticas.

- **Envíos de corrección de errores:** en el caso de las apps que ya están en el App Store o en métodos de distribución alternativos, las correcciones de errores ya no se retrasarán por infracciones de las directrices, excepto en los casos relacionados con cuestiones legales o de seguridad. Si tu app ha sido rechazada y cumple los requisitos para este proceso, usa App Store Connect para comunicarte directamente con el equipo de App Review para indicar que te gustaría aprovechar este proceso y que planeas abordar el problema en tu próximo envío.

¡Estamos deseando ver qué ingenias!

Última actualización: 13 de noviembre de 2025