

Guía de seguridad para trabajar con Grok Bot

Permisos mínimos, ordenador compartido, credenciales, aprobaciones, ejecución local y datos personales explicados para usuarios no técnicos.

Por qué esta guía

Un Bot que trabaja en tus herramientas puede hacer cosas reales: enviar, publicar, borrar, comprar. Por eso la seguridad no es un apartado opcional al final, sino la forma de trabajar desde el primer día. Esta guía resume lo que dice la documentación oficial de Grok Bot y añade recomendaciones prudentes. No es asesoramiento legal.

1. Permisos mínimos

- Conecta solo las herramientas que el trabajo necesita.
- Si el servicio lo permite, usa cuentas de servicio con permisos acotados o de solo lectura.
- Empieza por tareas de lectura y borradores.
- Mantén detrás de una aprobación: enviar, publicar, comprar, borrar y cambios en sistemas de producción.
- Revisa con regularidad los conectores instalados y las rutinas activas.

2. Un solo ordenador para todos tus Bots

Este es el punto que más se malinterpreta. Todos los Bots de tu cuenta usan **el mismo ordenador en la nube**, asignado a tu usuario y no a cada Bot. Eso significa que:

- Las cookies y sesiones iniciadas del navegador se comparten.
- Los archivos son visibles para todos los Bots.
- Las credenciales de la línea de comandos se comparten.
- Los conectores instalados son de toda la cuenta.

Cada Bot tiene su propia pantalla, pero la documentación es clara: **las pantallas son superficies de trabajo, no fronteras de seguridad**. No uses Bots separados para separar accesos. Si una credencial o un archivo no debe estar al alcance de otro de tus Bots, no lo pongas en ese ordenador.

Según la documentación para equipos, el ordenador alojado es una máquina virtual por miembro y está en EE. UU. Tenlo en cuenta si vas a tratar datos personales (ver apartado 6).

3. Contraseñas, códigos y CAPTCHAs: los escribes tú

Nunca pegues una contraseña ni un código de un solo uso en el chat normal. Cuando el Bot necesite una contraseña, una llave de acceso, un código de verificación en dos pasos, un CAPTCHA o una confirmación de pago:

1. Elige tomar el control en la petición del chat («Take over» en la interfaz en inglés) o abre el ordenador y toma el control.
2. Completa tú el paso sensible.
3. Indica que has terminado («I'm done») y dile al Bot que continúe.

Para algunas conexiones compatibles, el Bot puede presentar una petición segura de secreto: el valor queda oculto, fuera de la transcripción y no lo ve el modelo. No es un gestor de contraseñas general.

Las sesiones del navegador persisten y se comparten entre tus Bots: iniciar sesión para uno deja la sesión disponible para los demás. Algunas webs caducan la sesión o vuelven a pedir verificación; el Bot debe avisarte en lugar de intentar saltarse la comprobación.

4. Aprobaciones y «Auto Review»

Cuando una acción requiere aprobación, el chat muestra la operación propuesta y sus datos. Tienes tres opciones (rotuladas en inglés en la documentación): permitir una vez («Allow once»), permitir siempre («Always allow», que puede guardar una regla) y denegar («Deny»).

Lo que conviene saber:

- Una aprobación controla la acción propuesta; **no deshace lo que ya se ha hecho**.
- No apruebes nada cuyo destino o efecto no entiendas. Pide una explicación o un borrador.
- Las aprobaciones de trabajos que empezaron sin ti (una rutina, un disparador, un mensaje de otro Bot) caducan a los 10 minutos aproximadamente y la acción no se ejecuta.

Con «Auto Review» activado, Grok Bot evalúa las acciones antes de ejecutarlas. Puedes añadir reglas:

- **«Ask first»** (preguntar antes): detiene siempre las acciones que coinciden.
- **«Allow automatically»** (permitir automáticamente): deja pasar las que coinciden, salvo que la revisión automática encuentre otro motivo para parar.
- Si coinciden las dos, gana «Ask first».

Escribe reglas estrechas, por ejemplo «preguntar antes de enviar cualquier correo externo». Evita reglas amplias como «permitirlo todo en el navegador». La documentación recuerda que «Auto Review» se basa en un modelo y debe complementar, no sustituir, los permisos mínimos y las fronteras explícitas. Las reglas personales se guardan en el escritorio actual: otra instalación necesita las suyas.

5. Tu ordenador local es otra cosa

El ordenador en la nube de Grok Bot es distinto del Mac o el PC que tienes delante. Que un Bot ejecute órdenes en tu ordenador local es una capacidad aparte, que se controla en los ajustes («Execution on Local Computer»): preguntar cada vez (valor por defecto), permitir siempre o no permitir nunca.

Recomendación de la propia documentación: elige no permitir nunca, salvo que un Bot tenga un motivo concreto para trabajar con tus archivos locales.

6. Datos personales: prudencia

Esto no es asesoramiento jurídico; si tratas datos personales de clientes, empleados o contactos, consúltalo con quien lleve la protección de datos de tu negocio. Algunas pautas prudentes:

- Antes de adjuntar un archivo, quita los datos personales que no hagan falta.

- Ten presente que el trabajo se procesa en la nube de un tercero y que, según la documentación, el ordenador alojado está en EE. UU.
- La privacidad y el uso de datos se rigen por la configuración y las condiciones de la cuenta de Cursor; Grok Bot exige almacenamiento de datos y no admite el modo de privacidad antiguo («Legacy Privacy Mode»). Revisa las condiciones vigentes.
- Para captación comercial, respeta el RGPD, la normativa de comunicaciones comerciales y las condiciones de cada fuente. Investigar no es lo mismo que escribir a alguien.
- No pongas datos de clientes ni secretos en un Bot que vayas a compartir como plantilla: un enlace público muestra su configuración.

7. Cómo retirar accesos

Cuando un proyecto termina o un acceso ya no hace falta:

1. Pausa o borra las rutinas relacionadas.
2. Cierra la sesión en las webs del ordenador compartido.
3. Desinstala los conectores y revoca su autorización en el servicio de origen.
4. Borra los archivos sensibles de la carpeta de trabajo compartida (/workspace).
5. Oculta o borra los Bots que ya no deban aparecer.

Ojo: **borrar un Bot no borra los archivos ni las sesiones del ordenador compartido.**

8. En redes sociales y en X

Que un Bot pueda usar una web no garantiza que esa red permita la automatización. Publicar debe quedar siempre detrás de una aprobación. En X, los Bots pueden buscar y leer contenido público sin conectar tu cuenta (solo lectura). La función de mencionar a @bot en una publicación para encargar una tarea **no está disponible, por ahora, para cuentas de X con sede en la Unión Europea**, y por tanto tampoco en España.

Fuentes oficiales

- [Approvals, security, and privacy \(se abre en otra pestaña\)](#).
- [Use the computer and apps \(se abre en otra pestaña\)](#)
- [Security \(se abre en otra pestaña\)](#).
- [Grok Bot for teams and enterprises \(se abre en otra pestaña\)](#).
- [Tag @bot on X \(se abre en otra pestaña\)](#).

Máster en Agentes es una formación independiente, no afiliada ni respaldada por xAI. Comprobado con la documentación oficial el 20 de octubre de 2026; si algo ha cambiado, prevalece la documentación oficial.

Máster en Agentes es una academia independiente, no afiliada ni respaldada por xAI. La documentación oficial de Grok Bot prevalece si algo cambia. Versión del 2026-10-20.