

Tres skills para que no te hackeen la app que haces con Claude: una la audita como un hacker, otra vigila el código mientras Claude lo escribe y otra lo revisa antes de subirlo



1 · La auditoria de Cloudflare · la revisa como lo haría un hacker

Una skill gratis de Cloudflare (licencia MIT). Un agente prueba cada puerta de tu app buscando huecos y otro distinto intenta desmentir cada uno: si no aguanta la prueba, se descarta. Así solo te quedan los reales. No toca tu código: te deja un informe con qué arreglar primero.

Instálala:

```
npx skills@latest add cloudflare/security-audit-skill --skill security-audit -g -a
claude-code -y
```

Úsala:

```
/security-audit revisa mi app con el perfil quick
```

Ojo: Necesita Claude Code y Node.js, y gasta de tu plan de Claude. «quick» es la vuelta rápida; «standard» (la normal) y «deep» miran más a fondo. Si ya tienes otra skill que se llama security-audit, chocan.



2 · security-guidance · vigila el código mientras Claude lo escribe

Plugin oficial de Anthropic, para todos los planes. Mientras Claude escribe, busca patrones peligrosos en cada cambio, hace un repaso al final de cada turno y uno más a fondo en cada commit.

Instálalo en Claude Code:

```
/plugin install security-guidance@claude-plugins-official
```

Ojo: Es una capa más: avisa de lo que ve, pero lo importante lo revisas tú.



3 · /security-review · lo revisa antes de subirlo

Viene con Claude Code: no hay que instalar nada. Hace una pasada de seguridad sobre los cambios de la rama en la que estás, justo antes de subirlos.

Escríbelo en Claude Code:

```
/security-review
```

Ojo: Revisa lo que has cambiado, no la app entera. Para la app entera, la auditoría de Cloudflare.



Cuál usar, en una línea

¿La app que ya tienes? **Cloudflare** · ¿Mientras la haces? **security-guidance** ·
¿Antes de subir un cambio? **/security-review**



Lo que necesitas

Claude Code: en la pestaña Code de la app de Claude o en la terminal. Para la de Cloudflare, además, Node.js. Y la carpeta de tu app abierta en Claude Code. Ninguna de las tres cuesta dinero aparte: usan tu plan de Claude.

La auditoría de Cloudflare, paso a paso

Cinco pasos, de instalarla a cerrar la puerta más grave.



1. **Instálala sin abrir la terminal.** En la app de Claude, pestaña Code, pídele: «Ejecuta este comando» y pégale el de la página 1. Si te dice que falta Node.js, pídele que te explique cómo instalarlo. Después escribe / y busca /security-audit.
2. **Lánzala con una frase.** Abre la carpeta de tu app y escribe: /security-audit revisa mi app con el perfil quick. Solo lee tu código.
3. **Entiende el informe.** Pídele: «Explicame el informe como si no supiera programar: qué es cada hueco, qué podría pasar y cuál arreglo primero».
4. **Cierra la puerta más grave.** Pídele: «Arregla el hueco 1. Antes, escribe una prueba que demuestre el fallo, y después comprueba que ya no pasa».
5. **Pásala otra vez.** Según su propia página, una sola pasada encontró más o menos la mitad de lo que encontraron varias juntas. Tras arreglar, vuelve a lanzarla.



Antes de auditar, pégale esto a Claude

Voy a auditar la seguridad de mi app con /security-audit. Antes, sin cambiar nada, hazme una lista: qué partes guardan datos de clientes, dónde se inicia sesión, si hay claves o contraseñas escritas en el código y qué está abierto al público en internet. Explicámelo sin tecnicismos.



¿Tienes plan de pago? Claude Security

Plugin oficial de Anthropic: revisa tu repositorio o un cambio con varios agentes, otros agentes comprueban cada hallazgo y te propone el arreglo, que aplicas tú.

```
/plugin install claude-security@claude-plugins-official
```



Lo que no hace

Ninguna sustituye a todo lo demás: las propias guías de Anthropic dicen que son una capa más, que no reemplaza a los escáneres de dependencias ni al análisis estático. Si tu app cobra o guarda datos delicados, que la revise también una persona.



**Ningún proceso sin dueño.
Ninguna puerta sin candado.**

FUENTES: Cloudflare, security-audit-skill (github.com/cloudflare/security-audit-skill, licencia MIT). Anthropic, documentación de Claude Code: security-guidance (code.claude.com/docs/en/security-guidance), seguridad y /security-review (code.claude.com/docs/en/security) y Claude Security (code.claude.com/docs/en/claude-security). Consultado el 11 de octubre de 2026. Cloudflare es marca de Cloudflare, Inc.; Claude, de Anthropic. Esta chuleta no está hecha por ellos.