DIARIO DIGITAL DEV / RECURSO DE LECTURA

# ¿Afecta una vulnerabilidad a tu asistente de IA? Qué pedir al proveedor

Pide vincular el aviso con el componente y la versión realmente desplegados. La evaluación debe explicar su alcance, las condiciones de exposición, lo que falta comprobar y quién decide la respuesta. Si se corrige, exige evidencia de la nueva versión operativa y del funcionamiento del asistente después del cambio.

## Antes de aceptar la evaluación del proveedor

[ ] Identificar la versión y los entornos operativos.

[ ] Vincular el inventario de componentes con la entrega.

[ ] Contrastar paquete y versión con el aviso aplicable.

[ ] Registrar justificación, límites y responsables de la decisión.

[ ] Comprobar la corrección desplegada y los pendientes restantes.

## Próximas acciones

1. Elegir un asistente y confirmar quién identifica su versión operativa.
2. Pedir una evaluación que vincule inventario, aviso y contexto.
3. Acordar responsables y evidencia para cerrar o mantener cada pendiente.

## Notas para tu equipo

## Artículo y fuentes

https://www.digital-dev.cl/blog/vulnerabilidad-dependencia-asistente-ia-desplegado/


Agencia Nacional de Ciberseguridad de Chile: Asegurar equipos
https://anci.gob.cl/9basicos/asegurar-equipos/

OWASP CycloneDX: Software Bill of Materials (SBOM)
https://cyclonedx.org/capabilities/sbom/

OpenSSF: Open Source Vulnerability format
https://ossf.github.io/osv-schema/

OWASP CycloneDX: Vulnerability Exploitability eXchange (VEX)
https://cyclonedx.org/capabilities/vex/

Agencia Nacional de Ciberseguridad de Chile: Actualizar periódicamente
https://anci.gob.cl/9basicos/actualizar-periodicamente/