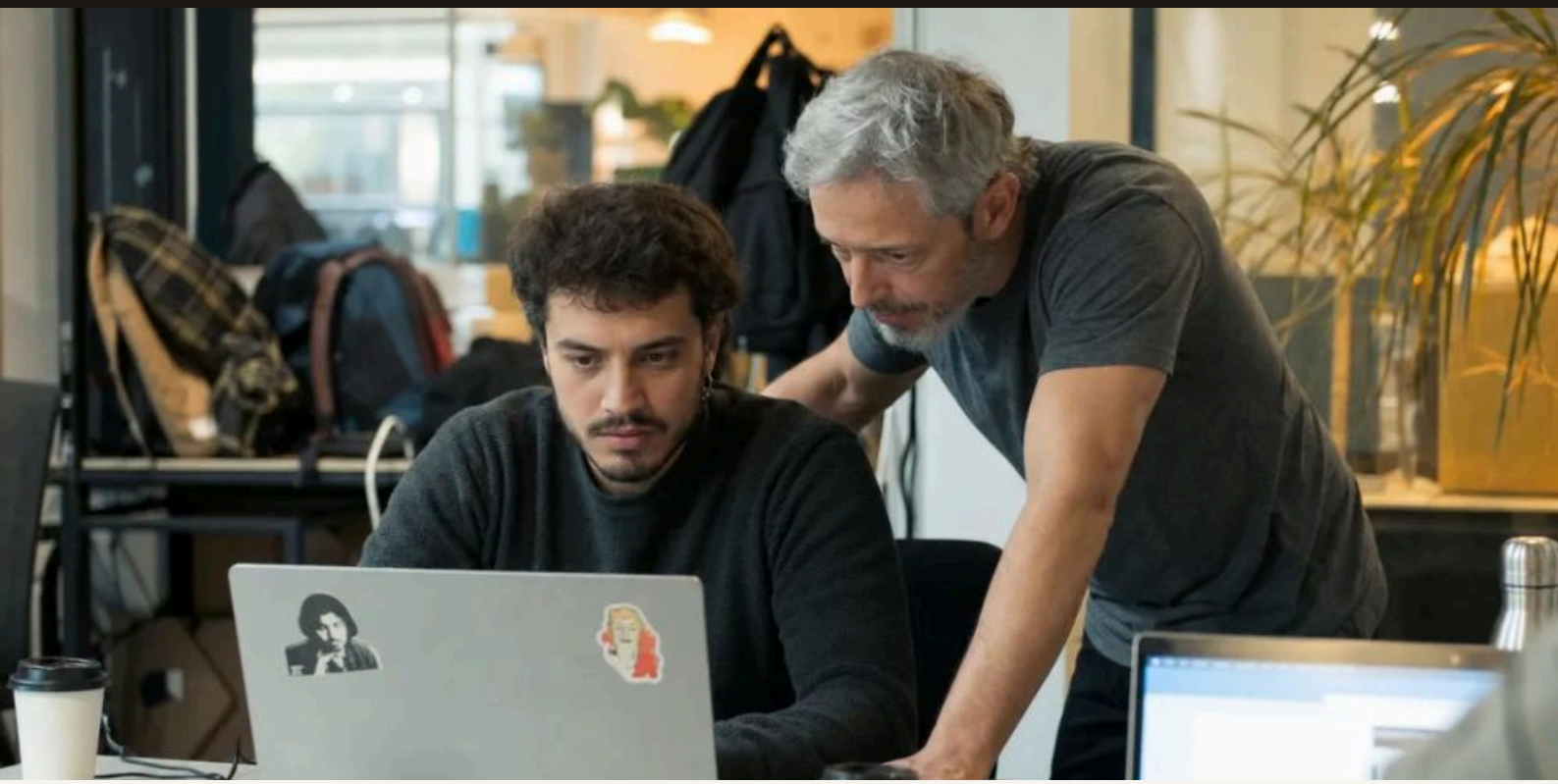

4 semanas | En vivo + material grabado · 15 cupos | Claude Code o Codex | Capacitación de seguridad informática

Revisión de seguridad de código con agentes de IA

Revisás tu propio código y tus dependencias con agentes de IA, y salís con chequeos automáticos que corren antes de cada publicación.

PARA QUIÉN

Programadores que publican su propio código y quieren encontrar fallas de seguridad antes de que las encuentre otra persona.

CÓMO TRABAJAN LOS AGENTES DE IA

Claude Code o Codex recorren tu repositorio y marcan hallazgos. Un segundo agente y otra persona los revisan por separado; vos decidís qué se corrige y comprobás que el arreglo funciona.

Cómo se cursa: Cada semana tenés material grabado para estudiar y practicar antes de la clase. La clase es en vivo y sirve de apoyo: resolvemos dudas, explicamos lo que se complica y enseñamos lo justo. Las clases en vivo no se graban.

Soporte incluido: Todas las capacitaciones incluyen 3 meses de soporte, ayuda y acompañamiento ante dudas, desde la última clase.

Lo que te llevas

- Un informe de hallazgos de tu propio repositorio, ordenado por gravedad.
- Reglas de acceso a datos y dependencias revisadas y corregidas.
- Secretos filtrados encontrados, rotados y bloqueados para que no vuelvan.
- Chequeos automáticos que corren antes de publicar.

Dicta Julián Bagilet

Más de 19 años en tecnología. Estudio de software en Villa General Belgrano, Córdoba.

Temario

1

SEMANA 1 SEGURIDAD

Secretos filtrados y configuración

Buscás claves en el código y en el historial, las rotás y bloqueás su regreso. Revisás la configuración de cada entorno.

QUÉ VEMOS

- Cómo una clave termina en el código: un archivo de prueba subido sin querer queda en el historial aunque después lo borres.
- Cómo buscar secretos en el código actual y en todo el historial con una herramienta, y qué hacer con cada hallazgo.
- Por qué borrar la clave del archivo no alcanza: hay que rotarla, es decir, invalidarla y crear otra nueva.
- Cómo bloquear que vuelva a pasar y revisar la configuración de cada entorno para que pruebas y producción no compartan claves.

Al terminar la semana: Terminás la semana con tus secretos expuestos rotados, un bloqueo que evita que vuelvan y la configuración de entornos revisada.

2

SEMANA 2 SEGURIDAD

Permisos y reglas de acceso a datos

Comprobás que cada usuario vea solo lo suyo, del lado del servidor. Revisás las reglas de acceso a la base de datos.

QUÉ VEMOS

- Qué es un acceso mal controlado: un usuario cambia el número en la dirección y ve el pedido de otra persona.
- Por qué la regla debe vivir en el servidor o en la base de datos: ocultar un dato en pantalla no impide pedirlo.
- Cómo leer las reglas de acceso de tu base de datos y detectar una que deja ver todas las filas a cualquier usuario.
- Cómo probar con dos cuentas tuyas que cada una ve solo lo propio, y dejar esa prueba escrita para repetirla.
- El laberinto de señuelos: tablas, funciones y claves trampa con datos inventados que ningún usuario real necesita. Si alguien las toca queda registrado con la hora del servidor y llega un aviso. Detectan y dejan evidencia, no contraatacan.

Al terminar la semana: Terminás la semana con tus reglas de acceso revisadas y corregidas, y una prueba con dos cuentas que podés repetir.

Temario (continuación)

3

SEMANA 3 SEGURIDAD

Dependencias, paquetes sospechosos y entradas

Auditás paquetes y versiones, detectás los dudosos y revisás qué datos entran sin validarse.

QUÉ VEMOS

- Qué es una dependencia y por qué tu proyecto confía en muchos paquetes de terceros que no escribiste.
- Cómo detectar un paquete sospechoso: nombre casi igual a uno famoso, publicado hace poco, sin repositorio claro o que ejecuta código al instalarse.
- Cómo auditar versiones con las herramientas del gestor de paquetes y decidir cuándo actualizar, fijar o quitar una dependencia.
- Qué es una entrada sin validar: un campo de formulario, un archivo subido o un parámetro de la dirección que tu código usa sin controlar.

Al terminar la semana: Terminás la semana con tus dependencias auditadas, los paquetes dudosos resueltos y una lista de las entradas que faltan validar.

4

SEMANA 4 SEGURIDAD

Revisor independiente y chequeos automáticos

Otro agente y otra persona revisan tu trabajo. Dejás chequeos automáticos que corren antes de cada publicación.

QUÉ VEMOS

- Por qué quien construye no debería aprobar: otro agente con otras instrucciones revisa y una persona lee su informe.
- Cómo ordenar los hallazgos por gravedad e impacto, y distinguir un falso positivo de un problema real.
- Cómo dejar chequeos automáticos que corren antes de publicar: escáner de secretos, auditoría de paquetes y pruebas de permisos.
- Cómo lograr que un chequeo que falla frene la publicación y avise con un mensaje claro de qué arreglar.
- Cómo dejar un agente vigilante con Claude que cada semana vuelva a revisar secretos, paquetes nuevos y reglas de acceso, y te mande el informe aunque nadie publique nada.

Al terminar la semana: Terminás con el informe final de tu repositorio y chequeos automáticos funcionando antes de cada publicación.

Seguridad y alcance

Seguridad incluida en esta capacitación

- Búsqueda de secretos en el código y en el historial, con rotación de lo expuesto.
- Revisión de dependencias y paquetes sospechosos antes de instalarlos.
- Revisión cruzada: el agente que construye no es el que aprueba.
- Reglas de acceso a datos comprobadas desde el servidor, no solo desde la pantalla.
- Entradas sin validar: dónde entran datos de afuera y cómo se controlan.
- Laberinto de señuelos con aviso y un agente vigilante programado que revisa cada semana.

Qué no se enseña ni se hace

- Probar o buscar fallas en código, servicios o sistemas ajenos.
- Armar ataques ni explotar fallas: se encuentran y se cierran en tu propio código.
- Saltear los términos de un proveedor o plataforma.

Requisitos

Necesitás experiencia previa programando y un repositorio propio para revisar. Hace falta un plan pago de Claude o de Codex (OpenAI), no incluido en el precio.

Inversión y formas de pago

Precio de la capacitación

$ 180.000

En vivo + material grabado · 15 cupos. Valores en pesos argentinos.

mercado pago

CUOTAS **3 cuotas de $ 60.000**
sin interés, con tarjeta, por Mercado Pago

TRANSFERENCIA **$ 153.000**
15% de descuento pagando por transferencia bancaria

Cómo inscribirte

1. **Escribinos**
Contanos qué querés lograr por WhatsApp.

2. **Confirmamos cupo y fecha**
Te avisamos apenas hay fecha y lugar en la cohorte.

3. **Reservá tu lugar**
Elegís cuotas o transferencia y recibís la confirmación por escrito.

WhatsApp +54 9 3546 54-6063

julianbagilet.com/capacitaciones/ · Instagram @mangopips_ok · Villa General Belgrano, Córdoba

Condiciones

Valores vigentes hasta el 31 de enero de 2027. Certificado de aprobación del estudio de Julián Bagilet, sin validez oficial. Derecho de arrepentimiento de 10 días corridos en compras a distancia por personas (Ley 24.240, art. 34). Si una cohorte no llega al mínimo de inscriptos, se reprograma o se devuelve el 100% de lo abonado. Los casos de las clases se explican como patrones, sin nombres ni datos de clientes.