



3 semanas

Hasta 15 participantes en talleres

Claude Code o Codex

✓ Capacitación de seguridad informática

Inventario y red team de la IA que su organización ya usa

Descubre qué IA usa cada área, con qué datos y qué puede hacer cada bot, y pruébalo con permiso.

PARA QUIÉN

Dirección, administración, tecnología y responsables de áreas de organizaciones donde la IA se adoptó área por área.

CÓMO TRABAJAN LOS AGENTES DE IA

Los agentes de IA (Claude o Codex, a elección de la organización) ayudan a ordenar el inventario y a preparar pruebas autorizadas sobre tus propios bots y conectores. Una persona del estudio revisa cada hallazgo, y otra de tu organización aprueba qué se prueba.

— Lo que te llevas

- ✓ Inventario de herramientas de IA, cuentas, datos y personas.
- ✓ Informe de hallazgos priorizados de las pruebas sobre tus bots, conectores y agentes.
- ✓ Mapa de flujos de datos: qué sale hacia dónde.
- ✓ Política de IA de una página y rutina trimestral para mantenerla al día.



Dicta Julián Bagilet

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

— Temario

1

SEMANA 1

Taller de inventario

Qué IA usa cada área, con qué cuentas y con qué datos. Plantilla de inventario y primer mapa de flujos de datos.

QUÉ VEMOS

- Cómo preguntar sin generar miedo: qué IA usas, con qué cuenta (personal o de la organización) y qué le pegas.
- Cómo anotar qué herramienta de IA usa cada área y con qué datos: planillas de clientes, contratos, facturas.
- La IA que apareció sola: funciones de IA dentro del correo, el CRM o el sistema de facturación que nadie activó a propósito.
- Cómo dibujar el mapa de flujos: de dónde sale cada dato, a qué servicio llega y quién puede verlo.

Al terminar la semana: Tu equipo termina con el inventario de IA por área completo y un primer mapa de hacia dónde viajan los datos.

2

SEMANA 2 SEGURIDAD

Permisos y pruebas autorizadas

Revisión de permisos y configuraciones, y pruebas adversariales autorizadas por escrito sobre los agentes y bots que ya tienes.

QUÉ VEMOS

- Qué puede leer, escribir o enviar cada bot o conector: el asistente que contesta mails quizá también podría borrarlos.
- Cuentas personales conectadas a datos de la organización y qué pasa cuando esa persona se va.
- Qué es una prueba adversarial, explicada simple: intentar engañar a tu propio bot con un texto malicioso para ver si obedece.
- Cómo se autoriza una prueba por escrito: qué se prueba, qué no, quién aprueba y qué se hace si algo falla.

Al terminar la semana: Tu equipo termina con los permisos revisados y las pruebas autorizadas por escrito, siempre sobre tus propios bots y conectores.

3

SEMANA 3 SEGURIDAD

Hallazgos, política y rutina

Hallazgos priorizados y arreglos. Redactamos la política de IA de una página y diseñamos la rutina trimestral.

QUÉ VEMOS

- Cómo se prioriza un hallazgo: qué es grave porque toca dinero o datos de clientes y qué puede esperar.
- Arreglos concretos: sacar permisos de más, separar cuentas personales, cambiar claves y retirar datos que no deberían estar.
- Qué significa "no verificado" y por qué es mejor admitirlo que dar por seguro algo que no se pudo probar.
- La política de IA de una página: qué se puede pegar, qué no, quién autoriza herramientas nuevas y cada cuánto se revisa.

Al terminar la semana: Terminan con el informe de hallazgos priorizados, la política de IA de una página y la rutina trimestral con fechas.

— Seguridad y alcance

✓ Seguridad incluida en este programa

- ✓ Qué datos se pegan hoy en una IA y cuáles no deberían pegarse nunca.
- ✓ Pruebas contra tus propios agentes, solo con autorización escrita.
- ✓ Los hallazgos graves se informan primero a quien decide.
- ✓ A qué cuenta apunta cada conector y qué puede leer o escribir cada bot.
- ✓ Lo que no se pudo verificar queda marcado como "no verificado".

— Qué no se enseña ni se hace

- ✗ Las pruebas se hacen solo sobre sistemas tuyos y con autorización escrita.
- ✗ No incluye pruebas de intrusión de red, certificaciones ni asesoramiento legal.
- ✗ Lo que un proveedor no autoriza probar no se prueba: queda como "no verificado".

— Requisitos

Una persona que conozca las cuentas y herramientas de cada área, y autorización escrita de la dirección. No hace falta programar.

— Inversión y formas de pago

Programa completo

\$ 6.500.000

Desde \$ 6.500.000, en pesos argentinos, hasta 15 participantes en talleres. Si el inventario es grande, se presupuesta por bloques. Anticipo del 50% al confirmar, saldo al finalizar.

Valores en pesos argentinos.



PAGO **Transferencia o Mercado Pago**

Anticipo del 50% al confirmar y saldo al finalizar. Se acuerda por escrito.

FACTURA Se emite factura por cada pago. El tratamiento de IVA se informa en la propuesta.

— Cómo inscribirte

1

Escribenos

Cuéntanos qué quieres lograr por WhatsApp.

2

Confirmamos cupo y fecha

Te avisamos apenas hay fecha y lugar en la cohorte.

3

Reservas tu lugar

Eliges cuotas o transferencia y recibes 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.