

5 semanas con ejercicio de incidente | Hasta 10 participantes | Claude Code o Codex

Capacitación de seguridad informática

Seguridad técnica de bots, agentes y automatizaciones de tu inmobiliaria

Tu equipo audita y ataca en un entorno de prueba su propio bot de WhatsApp, sus agentes y sus flujos, y los deja con pruebas automáticas, topes de gasto y un plan de incidente.

PARA QUIÉN

Inmobiliarias de cuatro a veinte personas, con su responsable técnico o proveedor, que ya usan o van a usar bots, agentes o automatizaciones con datos de clientes.

CÓMO TRABAJAN LOS AGENTES DE IA

Un agente de IA (Claude o Codex) arma el entorno de prueba y corre herramientas abiertas contra copias de tus sistemas con datos ficticios. Nada se ataca fuera de ese entorno, y todo alcance consta por escrito.

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

Lo que te llevas

- Un inventario de cada bot, agente y automatización que tiene tu inmobiliaria, con qué datos toca y con qué permisos.
- Webhooks, claves y accesos corregidos, y flujos de n8n o similares actualizados y con autenticación.
- Un plan de incidente practicado en un ejercicio con el equipo.
- Un informe de prueba contra una copia de tu bot, con hallazgos ordenados por gravedad.
- Una suite de abuso que se corre sola y bloquea un cambio si empeora algo.



Dicta Julián Bagilet

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

Temario

1

SEMANA 1 SEGURIDAD

Inventario y alcance autorizado

Listamos todo lo que tu inmobiliaria automatiza y fijamos por escrito qué se prueba y qué no.

QUÉ VEMOS

- Qué bots, agentes, flujos, scripts y accesos hay hoy, incluidos los que armó alguien del equipo por su cuenta: la IA en las sombras.
- Para cada uno: qué datos toca, qué puede leer, escribir o enviar, y quién lo mantiene.
- El alcance autorizado: se prueban solo copias de tus sistemas, con datos ficticios, y con permiso escrito de la dirección. El artículo 153 bis del Código Penal sanciona el acceso sin autorización o excediéndola.
- La lista OWASP para aplicaciones con modelos de lenguaje 2025 y la de agentes 2026 como vocabulario común del equipo.

Al terminar la semana: Tu equipo termina con el inventario, el orden de riesgo y el documento de alcance firmado por la dirección.

2

SEMANA 2 SEGURIDAD

Ataque a una copia de tu bot

Probamos el bot en un entorno de prueba: inyección directa e indirecta, fuga de instrucciones y salidas peligrosas.

QUÉ VEMOS

- Inyección directa e indirecta contra una copia del bot, con una ficha o un PDF con texto oculto. Se mide cuánto cambia la respuesta.
- Exfiltración por una imagen o un enlace que arma el modelo, y cómo la política de seguridad del navegador y el bloqueo de imágenes externas la frenan.
- La salida del modelo es un dato no confiable: se valida con código antes de usarla en una consulta, un mensaje o una orden.
- Herramientas abiertas de pruebas de seguridad de modelos (garak, PyRIT, promptfoo) corridas sobre la copia, y lectura del informe.
- Por qué la protección no puede ser una lista de frases: el centro británico de ciberseguridad advirtió en diciembre de 2025 que el riesgo puede no eliminarse y se gestiona con diseño.

Al terminar la semana: Tu equipo termina con el informe de la prueba, los hallazgos ordenados por gravedad y los primeros arreglos.

Temario (continuación)

3

SEMANA 3 SEGURIDAD

Permisos, agentes y datos cruzados

Reducimos lo que cada agente puede hacer y probamos que un cliente no vea lo de otro.

QUÉ VEMOS

- Exceso de agencia: funcionalidad, permisos y autonomía de más. Se recorta cada agente al mínimo y se cambia la autorización al código.
- La regla de dos de Meta y la trifecta letal aplicadas a cada agente del inventario.
- Datos entre clientes: si varios usuarios comparten una base de búsqueda, un cliente puede recibir información de otro. Se prueba y se separa.
- Seguridad por fila y claves en tu base: la clave de servicio saltea las reglas y no puede estar en el navegador.
- Aprobación humana atada a la acción para lo que mueve dinero, borra o envía.

Al terminar la semana: Tu equipo termina con los permisos recortados, la prueba de aislamiento entre clientes aprobada y la lista de aprobaciones humanas definidas.

4

SEMANA 4 SEGURIDAD

Webhooks, n8n, claves y cadena de suministro

Cerramos las entradas de datos, actualizamos las herramientas de automatización y revisamos lo que instala el agente de código.

QUÉ VEMOS

- Webhooks de WhatsApp con la firma validada, y flujos con autenticación y lista de IP. Se prueba antes y después con envíos falsos.
- n8n y herramientas parecidas: varias vulnerabilidades críticas se publicaron entre 2025 y 2026 y una figura en el catálogo de explotadas de CISA. Un calendario de actualización.
- Claves y tokens: escáner de secretos, rotación y permisos mínimos. En agosto de 2025 tokens robados de una integración tercera sirvieron para exportar datos de instancias de Salesforce.
- Código que escriben los agentes: un estudio de Veracode de 2025 halló fallas de seguridad en el 45% de sus pruebas. Se revisa y se prueba antes de instalar.
- Paquetes inventados por la IA: se verifica que cada dependencia exista, tenga historia y sea del autor correcto antes de instalarla.

Al terminar la semana: Tu equipo termina con las entradas cerradas, las herramientas al día y una lista de verificación para cada dependencia nueva.

Temario (continuación)

5

SEMANA 5 SEGURIDAD

Gasto, registros, pruebas de abuso e incidente

Dejamos topes, alertas y pruebas automáticas, y cerramos con un ejercicio de incidente con todo el equipo.

QUÉ VEMOS

- Topes de gasto mensual y alertas en el proveedor de modelos, y topes por usuario y por conversación dentro del bot.
- Registros de cada llamada a una herramienta, de cada pedido bloqueado y de los intentos repetidos, con los datos personales tapados.
- Una suite de casos de abuso que corre con cada cambio y frena el despliegue si empeora algo.
- Responsabilidad: lo que dice tu bot puede obligarte, y los datos de clientes los cuidás vos (ley 25.326). Qué preguntas llevar a tu asesor legal.
- El ejercicio: un bot que empieza a filtrar datos y un token comprometido al mismo tiempo. Quién apaga, a quién se avisa y qué se cambia primero.

Al terminar la semana: Tu equipo termina con los topes y las pruebas corriendo, el plan de incidente practicado y la fecha de la próxima revisión.

Seguridad incluida en este programa

- ✓ Alcance autorizado por escrito: solo copias de tus sistemas con datos ficticios.
- ✓ Webhooks con firma, flujos con autenticación y herramientas actualizadas.
- ✓ Plan de incidente practicado con todo el equipo.
- ✓ Permisos mínimos por agente y autorización decidida por código y no por el modelo.
- ✓ Topes de gasto, registros y pruebas de abuso automáticas.

Qué no se enseña ni se hace

- ✗ Probar, atacar o entrar a bots, cuentas o sistemas que no sean de tu inmobiliaria y sin autorización escrita.
- ✗ No se arman mensajes de engaño ni se clonan voces y rostros, ni se publican paquetes con nombres falsos para probar ataques.
- ✗ No incluye asesoramiento legal, auditoría certificada ni garantías de que no habrá incidentes.

Requisitos

Participan la dirección, quien administra los sistemas (o su proveedor) y quienes manejan datos de clientes. Una cuenta de Claude o de Codex, a cargo de la inmobiliaria. Si usan un proveedor externo, se suma al alcance por escrito.

Inversión y formas de pago

Programa completo

$ 4.800.000

Precio del programa completo, en pesos argentinos, hasta 10 participantes. Anticipo del 50% al confirmar, saldo al finalizar. No incluye el plan pago de Claude o Codex.

Valores en pesos argentinos.

mercado pago

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. **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 56-6697

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.