

PROGRAMA DE SEIS SEMANAS PARA EQUIPOS TÉCNICOS

IA segura en el repositorio: programa de 6 semanas

Que el equipo desarrolle con IA y con controles que se pueden medir, antes y después

Seis semanas con un diagnóstico de las configuraciones de IA, el workshop completo, un informe para dirección con cinco acciones priorizadas y una segunda medición con los números del propio equipo. No prometo un porcentaje de mejora. Lo que cambie, lo dejo medido.

6

semanas, del diagnóstico a la revisión

2

mediciones: la inicial y la de la semana 6

5

fases, cada una con un entregable

90 min

de revisión remota en la semana 6

EL PROBLEMA DE PARTIDA

Un día de formación cambia lo que el equipo sabe, pero lo que hace no siempre.

Al volver de un workshop, cada uno vuelve a su rama, a su plazo y a sus hábitos. Si nadie mira qué se aplicó, a las tres semanas queda un buen recuerdo y pocas configuraciones cambiadas. Con IA pesa más: los asistentes, los servidores MCP y los modos de autonomía se actualizan cada pocos meses y lo que se decidió ayer caduca.

Hay un segundo problema: la sensación de ir más rápido no es una medida. En 2025 un ensayo aleatorizado de METR con desarrolladores experimentados midió que tardaban más con IA y que ellos creían haber ido más rápido. Por eso mido al principio y al final en vez de prometer cómo irá.

El programa junta tres cosas que suelen compararse por separado: el día de formación, el seguimiento posterior y la evidencia que pide quien audita. Al final, la empresa tiene cambios en el repositorio, un informe que enseñar a dirección y dos mediciones para compararlas.

Cinco fases en seis semanas

01 Diagnóstico y medición inicial

Semana 0. Encuesta al equipo, revisión de sus configuraciones de IA y los primeros indicadores.

02 Workshop y evidencia

Semana 1. Workshop de 5 a 8 horas según el equipo, con los laboratorios adaptados a su stack y el paquete de evidencia.

03 Informe a dirección

Semana 2. De tres a cinco páginas con cinco acciones priorizadas y un responsable por acción.

04 Dudas y revisión de pull requests

Semanas 1 a 5. Un canal para preguntarme, con fecha de cierre, y revisión escrita de dos o tres pull requests reales.

05 Revisión y segunda medición

Semana 6. Noventa minutos en remoto y la comparativa del antes y el después.

Cinco fases y un entregable en cada una, de la medición inicial a la segunda medición.

Cinco resultados que se pueden enseñar a quien decide

Cada resultado tiene un entregable concreto y una semana en la que aparece. Lo que no puedo prometer es cuánto valdrán los indicadores. Eso depende de los datos del equipo.

01

Saber desde qué punto parte el equipo

Con una encuesta de diez minutos al equipo y la revisión de las configuraciones de IA que ya hay en los repositorios, queda por escrito qué lee el asistente, qué tiene conectado y qué puede ejecutar.

Prueba: ficha de diagnóstico y medición inicial con 4 a 6 indicadores acordados.

02

Salir del workshop con controles en el repositorio

En el último bloque cada participante aplica los controles sobre el código de la empresa. Las configuraciones quedan en una rama de su repositorio y la fusiona el equipo.

Prueba: rama con configuraciones, política técnica de uso de IA y MCP, y Definition of Done.

03

Tener evidencia para el control y algo más que el recuerdo de un curso

Asistencia firmada, certificado individual y un temario mapeado a las normas que apliquen a la empresa, con una carta de una página para quien audite.

Prueba: paquete de evidencia entregado la misma semana del workshop.

04

Darle a dirección un documento que se pueda leer

Qué se vio, qué se trabajó, qué riesgos aparecieron en las configuraciones y cinco acciones con responsable. No es una auditoría y el informe lo dice en la primera página.

Prueba: informe de 3 a 5 páginas en la semana 2.

05

Comprobar qué se aplicó de verdad

A las seis semanas repetimos los indicadores y vemos con el equipo qué se mantiene, qué se abandonó y qué hay que ajustar.

Prueba: comparativa del antes y el después con los números del equipo.

Qué pasa cada semana y quién lo hace

Casi todo el trabajo lo hago sin que el equipo tenga que parar. Pido tiempo en dos momentos: la encuesta, de diez minutos por persona, y el día del workshop.

Semana 0

Diagnóstico y medición inicial

El equipo contesta una encuesta de diez minutos. Yo miro las configuraciones de IA que ya hay en los repositorios y acordamos entre cuatro y seis indicadores. Con eso adapto los laboratorios al stack del equipo.

Entregable: Ficha de diagnóstico y medición inicial.

Semana 1

Workshop y paquete de evidencia

Doy el workshop completo, de 5 a 8 horas según el equipo, con el último bloque sobre el repositorio de la empresa. Cada participante firma la asistencia y al acabar el día preparo la evidencia del curso.

Entregable: Rama con configuraciones, política técnica de uso de IA y MCP, paquete de evidencia.

Semana 2

Informe a dirección

Escribo un documento de tres a cinco páginas para quien decide, con lo que salió en el diagnóstico, lo que trabajamos en el workshop y cinco acciones priorizadas con un responsable propuesto para cada una. No es una auditoría.

Entregable: Informe de 3 a 5 páginas.

Semanas 1 a 5

Canal de dudas y revisión de pull requests

Abrimos un canal en el Slack o Teams de la empresa y respondo en dos días laborales. El equipo me manda dos o tres pull requests reales y los comento por escrito, en la plataforma de la empresa y con sus permisos, o con fragmentos si la empresa lo prefiere. El canal se cierra al terminar la semana 5.

Entregable: Revisión escrita de dos o tres pull requests.

Semana 6

Revisión remota y segunda medición

Noventa minutos en remoto con el equipo para ver qué se aplicó, qué no y por qué. Repetimos los indicadores y ajustamos las configuraciones que lo necesiten.

Entregable: Comparativa del antes y el después.

La semana 1 es el workshop completo. Su temario, prácticas y agenda están en danielalfocea.com/formacion/workshop-desarrollo-seguro-con-ia

Cómo saber si ha servido

En 2025 un ensayo aleatorizado de METR con desarrolladores experimentados de código abierto midió que tardaban un 19 % más con IA y que ellos creían haber ido un 20 % más rápido. Son herramientas de principios de 2025 y no dice nada de un equipo concreto, pero enseña que la impresión no vale como medida. Por eso no prometo un porcentaje. Elegimos juntos los indicadores que sirvan a la empresa, y estos son candidatos.

Pull requests con código generado revisados con la lista

Qué parte de los cambios hechos con asistente pasa por la lista de revisión acordada.

Hallazgos de SAST y de secretos por pull request

Lo que ya detectan las herramientas del equipo, contado antes y después, sobre el mismo tipo de cambios.

Tiempo de revisión de un pull request generado

Cuánto tarda una persona en aceptar o rechazar, medido en el sistema de control de versiones de la empresa.

Cambios en la configuración del asistente que pasan por revisión

Cuántas modificaciones de ficheros como mcp.json o los ajustes del IDE tienen revisión humana.

Inventario de MCP y Skills con responsable y justificación

Cuántos de los conectados tienen alguien que responda de ellos.

Confianza del equipo en el código generado

Una encuesta corta, repetida en la semana 6. Es una percepción y la trato como tal.

Curso o programa

NECESIDAD	WORKSHOP	PROGRAMA
Que el equipo aprenda a usar los asistentes con controles	Con el curso vale: entre 5 y 8 horas según el equipo, con el último bloque sobre el código de la empresa.	Añade diagnóstico previo y revisión posterior.
Una justificación documentada de la formación para una norma o una auditoría	El curso incluye el paquete de evidencia.	Suma el informe a dirección y la comparativa final.
Saber qué se aplicó y qué cambió al cabo de unas semanas	El curso no lo cubre. Eso lo decide la empresa.	Dos mediciones y una revisión a las seis semanas.
Un equipo que va a aplicar los controles solo y tiene tiempo para hacerlo	Es lo que hace falta. Si el equipo se atasca, la garantía de los 30 días cubre una hora.	No hace falta.

LO QUE SE QUEDA EN LA EMPRESA

Lo que queda en la empresa seis semanas después

Además de todo el material del workshop, el programa deja documentos hechos para que circulen dentro de la empresa.

Ficha de diagnóstico

Cómo están las configuraciones de IA al empezar y lo que contesta el equipo en la encuesta.

Informe a dirección

De tres a cinco páginas con cinco acciones priorizadas y quién responde de cada una.

Revisión escrita de dos o tres pull requests

Comentarios sobre cambios reales del equipo, con las pautas del workshop.

Medición inicial y final

Una plantilla con los indicadores que elijamos juntos, rellena en la semana 0 y repetida en la 6.

Paquete de evidencia

Asistencia firmada, certificados individuales, temario mapeado y carta de una página para el auditor.

Comparativa del antes y el después

Lo que se midió, lo que cambió y lo que no, tal cual.

QUÉ INCLUYE

Todo lo del curso, y el resto del programa encima

El programa incluye el workshop y los cuatro bonus que van con él. Para explicar internamente qué incluye, esta lista es el mejor punto de partida.

+1

Paquete de evidencia de cumplimiento

Asistencia firmada, certificado individual con fecha, horas y contenidos, temario mapeado a las normas que apliquen a la empresa y carta de una página para el auditor.

+2

Encuesta previa de diez minutos al equipo

Me sirve para adaptar los laboratorios al stack del equipo y es la base de la medición inicial.

+3

Configuraciones en una rama del repositorio de la empresa

Las dejo en el último bloque, junto con una plantilla técnica de política de uso de IA y MCP. Es técnica y no jurídica, así que la adapta el equipo legal de la empresa.

+4

Repositorio de laboratorios con soluciones

Para repetirlos con quien se incorpore, con licencia de uso interno durante 12 meses.

CUMPLIMIENTO

Qué evidencia deja el programa y para qué controles sirve

El paquete sirve como evidencia para estos controles, pero no los cumple por sí solo. El control lo ejecuta y lo mantiene la empresa, y aquí se documenta la formación. En la llamada indico cuáles aplican a la empresa.

NORMA	QUÉ PIDE	QUÉ DEJO COMO EVIDENCIA
PCI DSS 4.0 · 6.2.2	Formación documentada, al menos cada 12 meses, para quien desarrolla software a medida, en seguridad relevante para su función y sus lenguajes.	Temario mapeado a los puntos del requisito, asistencia firmada y fecha.
ISO 27001:2022 · A.6.3	Concienciación, educación y formación en seguridad adecuadas a la función de cada persona.	Registro por persona y rol, con contenidos y fecha.
ISO 27001:2022 · A.8.25 y A.8.28	Ciclo de vida de desarrollo seguro y codificación segura, con formación de los desarrolladores.	Temario mapeado, Definition of Done y lista de revisión resultantes.
SOC 2 · CC1.4 y CC2.2	Programa de formación documentado, con registro de finalización por persona y profundidad según el rol.	Lista con nombre, fecha, contenido y rol, y certificado individual.

NORMA	QUÉ PIDE	QUÉ DEJO COMO EVIDENCIA
DORA · art. 13(6)	Formación en resiliencia operativa digital proporcional a la función, para entidades financieras sujetas al reglamento.	Registro de la formación y temario, para el expediente de la empresa.
AI Act · art. 4	Medidas para apoyar la alfabetización en IA del personal, adaptadas a su función y contexto. Es una obligación de medios y no exige certificado.	Registro interno de la formación, con contenido sobre riesgos y uso de IA según la función.

A QUIÉN VA DIRIGIDO

Para equipos que quieren ver qué ha cambiado y no quedarse en haber asistido

Encaja especialmente con

- Responsables de arquitectura de seguridad, AppSec y Platform Engineering que necesitan enseñar resultados a dirección.
- Empresas con PCI DSS, ISO 27001, SOC 2 o DORA donde la formación ya hay que documentarla.
- Engineering managers que ven código generado en producción y quieren saber en qué punto está su equipo.
- Equipos que usan Claude Code o GitHub Copilot y deciden los permisos caso por caso.

No es la formación adecuada si

- La empresa busca una charla de inspiración para todo el departamento.
- El objetivo es formar a doscientas personas. Para eso, una plataforma de formación sale más barata.
- El equipo aún no ha usado un asistente sobre un repositorio real.
- Lo que hace falta es una auditoría del código con informe de vulnerabilidades, o un certificado de cumplimiento de una norma.

Seguridad y desarrollo contados por alguien que ha trabajado en los dos lados



Soy Daniel Alfocea y llevo veinte años en desarrollo y seguridad. En Banco Santander fui Principal Engineer del departamento de IA cuando se puso en marcha el área. En BBVA fui Tech Lead de ciberseguridad. En 42Crunch, en Reino Unido, fui responsable de uno de sus productos de seguridad de APIs.

He presentado investigación en RSA Conference y en OWASP AppSec EU, y he sido ponente habitual de RootedCON. El Instituto Nacional de Ciberseguridad (INCIBE) me ha llamado varias veces como juez de sus concursos. Fundé Navaja Negra y el capítulo de OWASP Madrid. Soy autor de herramientas de seguridad muy usadas, como GoLismero, Plecost y Dockerscan, y de LAPIS, una investigación publicada en arXiv sobre cómo describirle una API a un modelo con menos tokens. Con Alfonso Muñoz escribí *MCP Seguro. Guía práctica para desarrolladores, arquitectos software y tech leads*.

Este programa lo hago yo de principio a fin, del diagnóstico a la revisión de la semana 6. Los pull requests también los reviso yo y no se los paso a nadie.

GARANTÍAS

Lo que garantizo, por escrito

Si las configuraciones no funcionan, las arreglo

Si las configuraciones que dejo en el repositorio de la empresa no funcionan, hago una sesión remota gratuita para corregirlas.

Una hora más si a los 30 días el equipo sigue atascado

Si a los 30 días el equipo se ha atascado aplicando algo del programa, le dedico una hora en remoto, gratis.

Esto no es una auditoría y no prometo porcentajes, ni menos vulnerabilidades ni más productividad. Lo que dejo medido es el antes y el después del equipo.

Preguntas que mejor resolver ahora

¿Qué diferencia hay con el workshop?

El workshop es la jornada presencial, de 5 a 8 horas según el equipo, y va dentro del programa. Lo que se suma es lo de antes y lo de después: el diagnóstico, la medición, el informe para dirección, el seguimiento y la revisión de la semana 6.

¿Qué tiempo nos pide a nosotros?

Diez minutos por persona para la encuesta, el día del workshop, la revisión de noventa minutos de la semana 6 y el tiempo que el equipo quiera dedicar a mandarme pull requests y dudas. Nada más.

¿Revisas nuestro código?

Reviso dos o tres pull requests que el equipo me mande, en la plataforma de la empresa y con sus permisos, o con fragmentos si la empresa lo prefiere. ¿Y el último bloque del workshop sobre su repositorio? Normalmente sí. Si la empresa no puede abrir su código ese día, trabajamos sobre un repositorio de práctica parecido a su stack. No es una auditoría ni hay informe de vulnerabilidades.

¿Qué pasa si los indicadores no mejoran?

Lo cuento igual. Mido para saber qué pasó y no para demostrar que ha funcionado. Si algo no se movió, en la revisión de la semana 6 miramos por qué y qué ajustar.

¿Cuánto cuesta?

Depende de la duración y del tamaño del equipo. Después de la primera conversación preparo una propuesta cerrada.

¿Incluye certificado?

Cada participante recibe un certificado individual con fecha, horas y contenidos. No hay examen y no es una acreditación oficial.

¿Qué normas cubre el paquete de evidencia?

Sirve como evidencia de formación para PCI DSS 4.0 (6.2.2), ISO 27001, SOC 2, DORA y el artículo 4 del AI Act. No certifica el cumplimiento de ninguna, porque el control lo ejecuta la empresa. Antes de empezar digo cuáles tienen sentido en cada caso.

¿Se puede bonificar por FUNDAE?

Al pedir fecha paso la información que necesita la gestoría o el departamento de formación.

¿Garantiza que no tendremos incidentes con IA?

No. Lo que garantizo son las fases descritas, la entrega de los documentos y las dos garantías de arriba. Que baje el riesgo depende de que la empresa aplique y mantenga los controles después.

FORMATO

Un equipo, seis semanas y una propuesta cerrada

El precio depende de la duración y del tamaño del equipo, y lo cerramos tras una llamada, según el stack, el número de repositorios y los indicadores que elija la empresa. Incluye el diagnóstico, el workshop, el paquete de evidencia, el informe, el seguimiento y la segunda medición.

- Participantes del mismo equipo o de áreas que trabajan juntas.
- Diagnóstico, workshop, paquete de evidencia, informe, seguimiento y revisión final.
- En español o en inglés.
- Sala, pantalla y wifi a cargo de la empresa el día del workshop. El resto es en remoto.
- Desplazamiento fuera de Madrid acordado antes de cerrar la fecha.

Escríbeme a

yo@danielalfocea.com

En la llamada vemos si el programa encaja, qué fechas hay y qué indicadores tiene sentido medir en el equipo.

Bonificable a través de FUNDAE.

CORREO

yo@danielalfocea.com

PROGRAMA EN LA WEB

danielalfocea.com/formacion/programa-desarrollo-seguro-con-ia