

PROGRAMA DE 6 SEMANAS PARA EQUIPOS TÉCNICOS

OWASP en el código del equipo: programa de 6 semanas

Seis semanas que dejan el repositorio cambiado y la mejora medida con números.

Primero mido dónde está el equipo. Luego imparto el workshop de desarrollo seguro, reviso por escrito pull requests reales del equipo y en la semana 6 vuelvo a medir. La empresa se queda con los controles puestos en su repositorio, la evidencia para el auditor y un antes y un después con los números del propio equipo.



6

semanas, de la medición inicial a la revisión final

90 min

de revisión remota en la semana 6

5

fases, cada una con un entregable

4 a 6

indicadores acordados con el equipo

EL PROBLEMA DE PARTIDA

El equipo sale del curso con ganas y a las tres semanas el código es el de siempre

Si la formación es un solo día, lo aprendido tiene que competir con el sprint, las entregas y las incidencias. El control de acceso roto, la inyección o los secretos en el historial de git se quedan donde están por mucho que el equipo los entendiera un martes. Se van cuando alguien los busca en el código, los arregla y deja un test para que no vuelvan.

Y a quien pide formación le suelen pedir que la demuestre. Si la empresa vende a bancos, trata pagos, tiene ISO 27001 o pasa una auditoría SOC 2, la formación de desarrolladores tiene que estar documentada, con fecha, contenido y asistentes. Con una lista de asistencia a veces no llega.

El programa cubre las dos cosas. Mido el punto de partida, paso del workshop al repositorio de la empresa revisando cambios reales y acabo volviendo a medir, para que quien decide vea qué se movió y qué no.

Las cinco fases del programa

01 Diagnóstico y medición inicial

Semana 0. Encuesta de 10 minutos al equipo, muestra del código de la empresa y 4 a 6 indicadores acordados.

02 Workshop presencial (5 a 8 horas según el equipo)

Semana 1. Los laboratorios adaptados al stack del equipo y la última parte del día sobre el repositorio de la empresa.

03 Evidencia e informe a dirección

Semanas 1 y 2. Paquete de evidencia para el auditor e informe de 3 a 5 páginas con 5 acciones priorizadas.

04 Dudas y revisión de pull requests

Semanas 1 a 5. Un canal para preguntarme, con fecha de cierre, y revisión escrita de 2 o 3 pull requests del equipo.

05 Revisión y segunda medición

Semana 6. Noventa minutos en remoto y la comparativa con la medición inicial.

Cinco fases y un entregable en cada una. Al final queda una comparativa con los números del equipo.

RESULTADO DEL PROGRAMA

Qué tiene la empresa al terminar la semana 6

Todo esto se puede enseñar a quien tenga que aprobarlo. Ninguna parte depende de que yo prometa un porcentaje.

01

Un punto de partida medido

Indicadores que elegimos juntos sobre el código de la empresa y el pipeline del equipo, medidos antes de dar una sola hora de formación.

Evidencia: ficha de diagnóstico con los valores de la semana 0.

02

Controles puestos en el repositorio

En el último bloque del workshop dejo las configuraciones y la checklist de pull request en una rama del repositorio, y el equipo las revisa y las fusiona.

Evidencia: una rama con los cambios, en el repositorio de la empresa y con sus permisos.

03

Dirección con decisiones en la mano, sin presentación de por medio

Entre tres y cinco páginas con lo que salió en el diagnóstico, lo que se trabajó y cinco acciones priorizadas, cada una con un responsable propuesto.

Evidencia: informe a dirección entregado en la semana 2. Ojo, no es una auditoría.

04

Revisión de pull requests reales

Dos o tres cambios del equipo revisados por escrito con las mismas pautas del workshop, para que el equipo vea cómo se aplican sobre su código y no sobre el de unas prácticas.

Evidencia: comentarios por escrito sobre los pull requests del propio equipo.

05

Un antes y un después con los números del equipo

Los mismos indicadores de la semana 0, medidos otra vez en la semana 6, con lo que se movió, lo que no y qué creo yo que ha pasado.

Evidencia: comparativa de la semana 0 contra la semana 6.

Seis semanas, cinco fases

Cada fase tiene un responsable (el equipo o yo) y un entregable. El programa incluye el workshop de desarrollo seguro completo, y su temario está en su propia ficha.

Semana 0

Diagnóstico y medición inicial

El equipo contesta una encuesta de 10 minutos sobre su stack, sus prácticas y sus dudas. Yo miro una muestra de código y de pipeline que el equipo me deje ver y acordamos entre 4 y 6 indicadores. Con todo eso adapto los laboratorios al stack del equipo.

Entregable: Ficha de diagnóstico con la medición inicial.

Semana 1

Workshop presencial (5 a 8 horas según el equipo)

Doy el workshop completo en las instalaciones de la empresa. El último bloque lo hacemos sobre el repositorio de la empresa y ahí dejo en una rama las configuraciones y la checklist de pull request. El equipo decide qué fusiona.

Entregable: Rama con configuraciones y checklist; certificados individuales.

Semanas 1 y 2

Evidencia e informe a dirección

Preparo el paquete de evidencia con la asistencia firmada el día del workshop. Con lo que salió en el diagnóstico y en el bloque sobre el código de la empresa escribo el informe para dirección, lo presento y lo comentamos.

Entregable: Paquete de evidencia e informe de 3 a 5 páginas con 5 acciones priorizadas.

Semanas 1 a 5

Canal de dudas y revisión de pull requests

Abrimos un canal en el Slack o Teams de la empresa. Respondo en dos días laborables y se cierra al final de la semana 5. El equipo me manda dos o tres pull requests que quiera revisar con las pautas del workshop y yo los comento por escrito.

Entregable: Comentarios escritos sobre 2 o 3 pull requests.

Semana 6

Revisión remota y segunda medición

Noventa minutos con el equipo para ver qué se ha aplicado, qué no y por qué, y ajustar las configuraciones si hace falta. Antes de la sesión repetimos la medición con los mismos indicadores de la semana 0.

Entregable: Comparativa entre la semana 0 y la semana 6.

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

Los indicadores los elegimos juntos y se miden dos veces

No prometo que el código vaya a tener un porcentaje menos de vulnerabilidades. Depende de lo que aplique el equipo y cualquier cifra que diera me la estaría inventando. Lo que hago es medir lo mismo antes y después, con los datos del equipo, y contar lo que se movió. Estos son los candidatos y elegimos entre cuatro y seis.

Hallazgos de SAST por pull request

Cuántos hallazgos nuevos entran en cada cambio, medidos sobre una ventana de pull requests anterior y otra posterior.

Pull requests revisados con la checklist de autorización

Qué proporción de los cambios que tocan endpoints pasa por la checklist del programa.

Secretos detectados en el repositorio y en su historial

Cuántos encuentra un escáner de secretos y cuántos se han rotado y retirado en la semana 6.

Dependencias con vulnerabilidad conocida y tiempo de corrección

Cuántas tiene el repositorio y cuánto tarda el equipo en actualizar las críticas.

Pipelines con lockfile y acciones fijadas por SHA

Qué proporción de los pipelines instala desde el lockfile y referencia las acciones por commit completo.

Confianza del equipo, por encuesta

Las mismas preguntas en la semana 0 y en la 6 sobre si saben revisar autorización, entradas y dependencias. Es una percepción y lo cuento como tal.

Curso o programa

NECESIDAD	WORKSHOP	PROGRAMA
Que el equipo aprenda a explotar y arreglar los fallos más repetidos.	Con el curso vale. Un día, seis laboratorios y el bloque sobre el código de la empresa.	Incluye el curso entero.
Saber si algo ha cambiado semanas después.	No mide nada. El equipo se lleva plantillas y la medición queda en manos del equipo.	Medición en la semana 0 y en la 6, con los mismos indicadores.
Que dirección vea qué hacer y en qué orden.	No lleva informe. Los hallazgos se quedan en el equipo.	Informe de 3 a 5 páginas con cinco acciones priorizadas.
Que el equipo aplique lo del workshop a su código, con alguien que lo revise.	Cada uno trabaja en su portátil durante el último bloque.	Canal de dudas y revisión escrita de 2 o 3 pull requests del equipo.

Entregables del programa

Todo pasa a ser de la empresa desde la semana en que se entrega. El material de laboratorio tiene licencia de uso interno durante 12 meses.

Ficha de diagnóstico

Lo que contesta el equipo en la encuesta, lo que veo en la muestra de código y los indicadores de la medición inicial.

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 una carta de una página para el auditor.

Revisión escrita de 2 o 3 pull requests

Comentarios sobre cambios reales del equipo, en la plataforma de la empresa o sobre fragmentos, lo que prefiera el equipo.

Repositorio de laboratorios con soluciones

ByteBazaar, los enunciados y las soluciones. Con licencia de uso interno durante 12 meses, para repetirlos con quien se incorpore.

Configuraciones y checklist de PR en una rama del repositorio

Checklist de autorización por endpoint y gates de CI adaptados al pipeline del equipo. Es una plantilla técnica y el equipo la revisa antes de fusionar.

Informe a dirección

De 3 a 5 páginas, con cinco acciones priorizadas y responsable propuesto para cada una.

Comparativa de la medición

Semana 0 y semana 6 con los mismos indicadores, y lo que yo vigilaría en los meses siguientes.

INCLUIDO EN EL PROGRAMA

Cuatro cosas que se quedan en la empresa además del trabajo de las seis semanas

Son las mismas que vienen con el curso. En el programa van metidas en las fases en lugar de ir sueltas.

+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 una carta de una página para el auditor.

+2

Encuesta previa al equipo

Diez minutos por persona en la semana 0 para adaptar los laboratorios al stack del equipo. Si no llega a tiempo, sigo con el temario estándar.

+3

Configuraciones en una rama del repositorio de la empresa

Gates de CI y checklist de pull request, que dejo en el último bloque del workshop. Es una plantilla técnica que revisa y fusiona el equipo.

+4

Repositorio de laboratorios con soluciones

Las prácticas del día para repetirlas con quien entre al equipo. Con licencia de uso interno durante 12 meses.

CUMPLIMIENTO

Qué evidencia deja el programa y para qué sirve

El programa deja la formación documentada. No certifica el cumplimiento de ninguna norma, eso lo valora el auditor, y este registro es una de las piezas que puede usar.

NORMA	QUÉ PIDE	QUÉ DEJO COMO EVIDENCIA
PCI DSS 4.0 · 6.2.2	Formación al menos cada 12 meses para el personal que desarrolla software a medida, en diseño seguro, codificación segura y herramientas de testing, documentada.	Temario mapeado a los puntos del requisito, asistencia firmada y certificado individual con fecha.
ISO/IEC 27001:2022 · A.6.3	Concienciación, educación y formación en seguridad adecuadas a la función de cada persona.	Registro por persona y por rol con contenidos y fecha.
ISO/IEC 27001:2022 · A.8.25 y A.8.28	Ciclo de desarrollo seguro y codificación segura, que incluye formar a quien programa.	Temario mapeado y la checklist de pull request y los gates de CI que quedan en la rama de la empresa.
SOC 2 · CC1.4 y CC2.2	Programa de formación documentado, con registros de finalización por empleado y profundidad según el rol.	Lista con nombre, fecha, contenido y rol, más el informe a dirección.
DORA · artículo 13(6)	Programas de formación en resiliencia operativa digital para el personal de entidades financieras, proporcionales a su función.	Registro de asistencia y temario, para quien está dentro del ámbito de DORA.

Para un equipo que quiere acabar con el repositorio cambiado y con números

Encaja especialmente con

- Equipos que mantienen aplicaciones web o APIs en producción.
- Tech leads y responsables de ingeniería a quienes les piden demostrar que el equipo está formado en desarrollo seguro.
- Empresas con PCI DSS, ISO 27001, SOC 2 o DORA en el horizonte, que necesitan documentar la formación de quien programa.
- Equipos que prefieren una comparativa de antes y después a una promesa.

No es la formación adecuada si

- La empresa busca una charla de inspiración para todo un departamento.
- El objetivo es formar a doscientas personas. Para eso sale más barata una plataforma de formación.
- Lo que hace falta es una auditoría o un pentest. Aquí el equipo busca en su propio código y no hay informe de hallazgos técnicos.
- Con una jornada basta. En ese caso, mejor el workshop de un día.

QUIÉN LO IMPARTE

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*.

La aplicación de los laboratorios es mía y es pública. Las seis semanas las llevo yo de principio a fin, de la medición inicial a la revisión final.

Lo que arreglo yo sin cobrar un euro

Configuraciones que no funcionan

Si las configuraciones que dejo en el repositorio de la empresa no funcionan en el pipeline del equipo, las arreglo en una sesión remota sin coste y repetimos la revisión de la semana 6.

Equipo atascado a los 30 días

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

Esto no es una auditoría y no prometo menos vulnerabilidades ni un porcentaje de mejora. Lo que dejo es el antes y el después, medidos con los números del equipo.

Preguntas que mejor resolver ahora

¿Qué parte es presencial?

El workshop, de 5 a 8 horas según el equipo. La encuesta, el diagnóstico, el canal, la revisión de pull requests y la sesión final van en remoto.

¿Ves o te llevas nuestro código?

Ve una muestra de código y de pipeline en la plataforma de la empresa, con sus permisos, para el diagnóstico y para revisar los pull requests que me mande el equipo. No me llevo copias. Si la empresa prefiere no darme acceso, trabajo con los fragmentos que elija.

¿Qué pasa si el equipo no responde a la encuesta?

Hay un plazo fijo. Si no llega a tiempo, sigo con el temario estándar y con los indicadores que se puedan medir sin la encuesta.

¿Quién decide los indicadores?

Los acordamos juntos en la semana 0, entre los seis candidatos de esta página u otros que tengan sentido en cada caso. Prefiero pocos y que se puedan medir de verdad.

¿El canal de dudas es soporte sin límite?

No. Es un canal en el Slack o Teams de la empresa. Respondo en dos días laborables y se cierra al final de la semana 5. Después queda la revisión de la semana 6.

¿El paquete de evidencia certifica que cumplimos PCI, ISO o SOC 2?

No. Es la documentación de la formación, que el auditor puede usar como evidencia de un control. Si el control se da por cumplido lo decide el auditor.

¿Se puede bonificar por FUNDAE?

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

¿Cuánto cuesta?

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

¿Se puede hacer también el workshop en remoto?

Sí, aunque en presencial va mejor para desatascar laboratorios y para el bloque sobre el código de la empresa. El alcance es el mismo.

¿Garantiza que no tendremos incidentes de seguridad?

No. Lo que garantizo son las fases y los entregables de esta página y las dos garantías de arriba. Que baje el riesgo depende de que el equipo aplique y mantenga los controles después.

FORMATO

Una propuesta cerrada, después de una conversación

El precio depende de la duración y del tamaño del equipo, y lo cerramos tras una llamada porque también cuentan el tamaño del código que haya que revisar y cuántos indicadores acordemos. Incluye el workshop completo, el paquete de evidencia, el informe a dirección, el canal de dudas, la revisión de pull requests, la revisión final y la segunda medición.

- Participantes del mismo equipo o de áreas que trabajan juntas.
- Workshop presencial en la empresa y el resto en remoto. En español o en inglés.
- Sala, pantalla, wifi y portátiles a cargo de la empresa, con Docker instalado y acceso al repositorio de cada participante.
- Acceso a una muestra de código y de pipeline para el diagnóstico, en la plataforma de la empresa y con sus permisos.
- Desplazamiento fuera de Madrid acordado antes de cerrar la fecha.

Escríbeme a

yo@danielalfocea.com

En la llamada vemos si el programa encaja, qué indicadores y qué fechas. Si con el curso de un día basta, lo digo.

Bonificable a través de FUNDAE.

CORREO

yo@danielalfocea.com

PROGRAMA EN LA WEB

danielalfocea.com/formacion/programa-desarrollo-seguro