qualoom®

Inspiring Technology
for People

Implementación Técnica de CI/CD Seguro: Buenas Prácticas y Herramientas

Área de Seguridad
Fecha 00/00/2025
Versión 1.0

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

01 CI/CD: aceleración, pero con seguridad integrada

02 El enemigo dentro del flujo

03 Checklist de un pipeline seguro

04 Tu stack DevSecOps comienza aquí

05 Seguridad como parte del sprint

06 Resultados tras implementar CI/CD seguro

07 Conclusión

qualoom®

Inspiring Technology
for People

Introducción.
CI/CD: aceleración, pero con seguridad integrada

La automatización del ciclo de vida de desarrollo y despliegue (CI/CD) es fundamental para incrementar la eficiencia, garantizar consistencia y reducir errores humanos. Sin embargo, la velocidad no debe comprometer la seguridad.

Este documento proporciona un compendio de buenas prácticas técnicas y herramientas orientadas a asegurar cada fase del pipeline CI/CD. La filosofía DevSecOps promueve integrar seguridad desde el inicio del ciclo de desarrollo, garantizando que los controles no ralenticen el flujo, sino que se conviertan en una capa de protección continua.

qualoom®

Inspiring Technology
for People

El enemigo dentro del flujo

Los pipelines CI/CD pueden ser un vector de riesgos si no se **aplican controles adecuados.**

Entre los riesgos más frecuentes se incluyen:

Dependencias no verificadas

Bibliotecas externas con vulnerabilidades conocidas.

Inyección de secretos

Exposición accidental de claves, tokens o credenciales.

Scripts maliciosos

Ejecución de código no confiable que compromete el entorno.

Permisos excesivos en runners

Usuarios o agentes con privilegios innecesarios.

Ausencia de validaciones antes del despliegue

Errores de código que llegan a producción.

qualoom®

Inspiring Technology
for People

Checklist de un **pipeline seguro**

Para minimizar riesgos, un pipeline seguro debe incorporar:

- **Escaneo de código previo a build,** SAST, linters y análisis de vulnerabilidades.
- Separación de entornos. Build, staging y producción aislados para contener errores.
- Separación de entornos. Build, staging y producción aislados para contener errores.
- Registros de auditoría. Trazabilidad completa de cada ejecución.
- Aprobaciones manuales en fases sensibles. Gates para despliegues críticos.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Tu stack DevSecOps comienza aquí

Al integrar seguridad en el pipeline, es crucial seleccionar herramientas que complementen cada fase:

Herramienta	Función principal	**Integración CI/CD**
Jenkins + OWASP Dependency Check	SAST y gestión de dependencias	Jenkins pipeline
GitLab CI + Secret Detection	Detección de secretos	GitLab runners
GitHub Actions + CodeQL	Análisis de código estático	Actions workflows
CircleCI + Terraform Compliance	Validación IaC	Pipelines automatizados

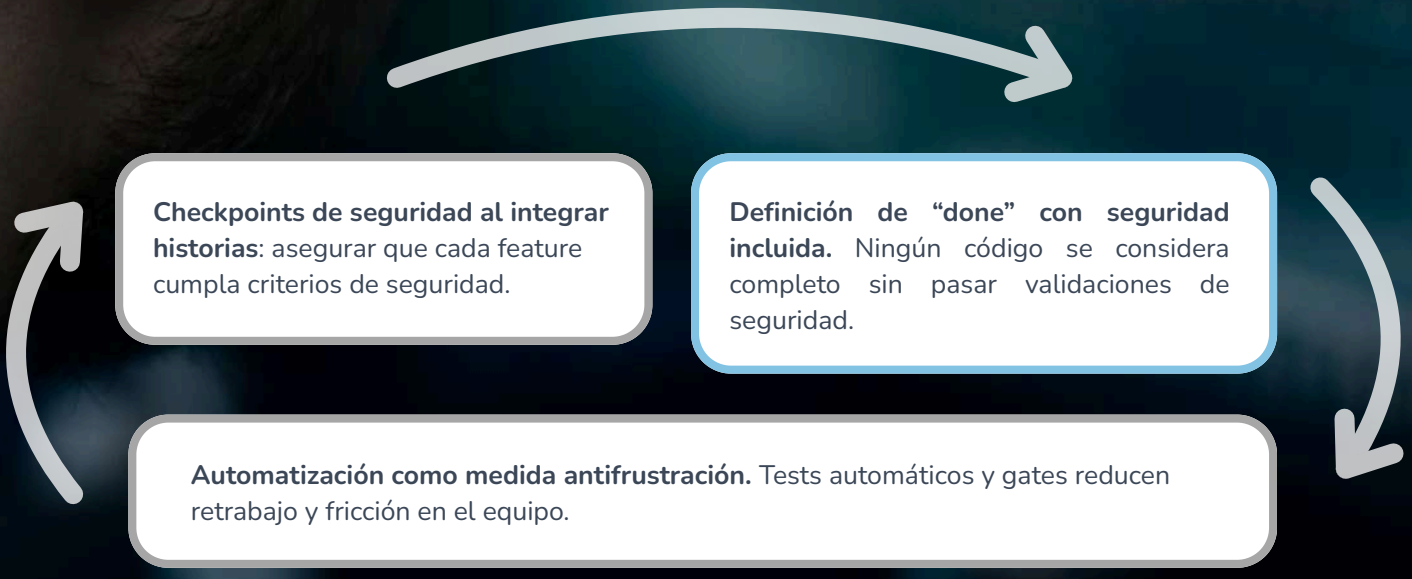
qualoom®

Inspiring Technology
for People

Seguridad como parte del **sprint**

La integración de la seguridad en metodologías ágiles requiere acciones específicas y recurrentes durante cada iteración. Estas prácticas aseguran que los equipos no vean la seguridad como una tarea aislada, sino como **parte de la definición de valor entregado en cada sprint.**

Algunas de las más efectivas son:



Checkpoints de seguridad al integrar historias: asegurar que cada feature cumpla criterios de seguridad.

Definición de "done" con seguridad incluida. Ningún código se considera completo sin pasar validaciones de seguridad.

Automatización como medida antifrustración. Tests automáticos y gates reducen retrabajo y fricción en el equipo.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Resultados tras implementar CI/CD seguro

Reducción de vulnerabilidades en despliegues

Hasta

72 %

- Al integrar análisis de código estático (SAST).
- Validaciones de dependencias.
- Pruebas dinámicas (DAST) directamente en el pipeline

Las vulnerabilidades se identifican y corrigen antes de alcanzar producción.

Repositorios libres de secretos.

La combinación de Git hooks, escáneres automáticos y el uso de gestores centralizados de secretos (vaults) **asegura que credenciales y claves no queden expuestas en repositorios ni pipelines.**

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Resultados tras implementar CI/CD seguro

Trazabilidad y auditoría continua

Cada ejecución del pipeline queda registrada, **permitiendo demostrar cumplimiento normativo** (ISO 27001, SOC 2, GDPR) y facilitando auditorías internas y externas.

Validaciones automatizadas antes del release.

la integración de security gates y pruebas de cumplimiento permite que solo los artefactos verificados avancen hacia producción, **garantizando despliegues consistentes y confiables.**

Mejor colaboración entre equipos.

La adopción de DevSecOps promueve una cultura de responsabilidad compartida donde **desarrollo, operaciones y seguridad trabajan bajo un mismo flujo.**

Más información www.qualoom.es

qualoom®

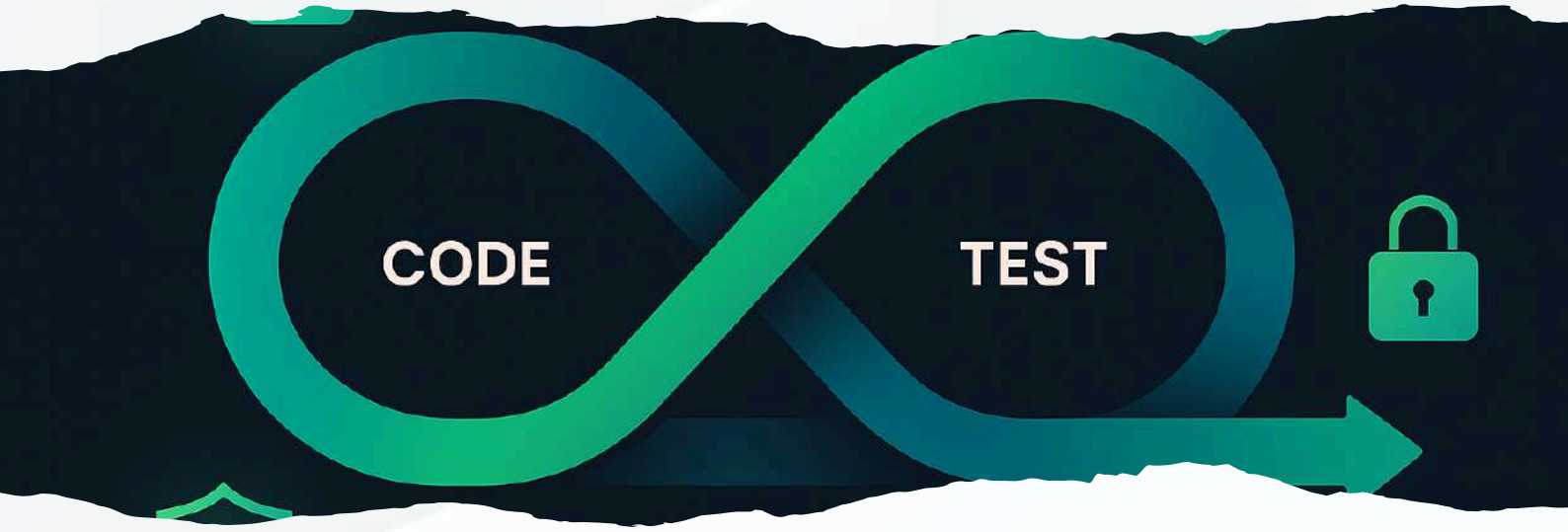
Inspiring Technology
for People

El pipeline es la nueva frontera de seguridad

Un pipeline inseguro constituye un punto crítico de exposición que puede comprometer tanto la integridad del software como la continuidad del negocio. Adoptar un enfoque DevSecOps desde la concepción del pipeline no es una opción, sino una necesidad estratégica.

Los beneficios de integrar seguridad desde el diseño incluyen:

- Reducción de riesgos y retrabajo: los problemas se detectan en fases tempranas, evitando costes elevados en producción.
- Mayor confiabilidad en despliegues: los entornos reciben únicamente artefactos validados y auditados.
- Aceleración del time-to-market: la seguridad automatizada permite mantener la velocidad sin sacrificar protección.



qualoom®

Inspiring Technology
for People

Asegura tu pipeline, **protege tu futuro digital.**

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es