qualoom®

Inspiring Technology
for People

Modelo de Madurez DevSecOps 2026: Estrategias para Integrar Seguridad en la Entrega Continua

Área de DevOps y DevSecOps
Fecha 17/03/2026
Versión 1.0
Clasificación: Público

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

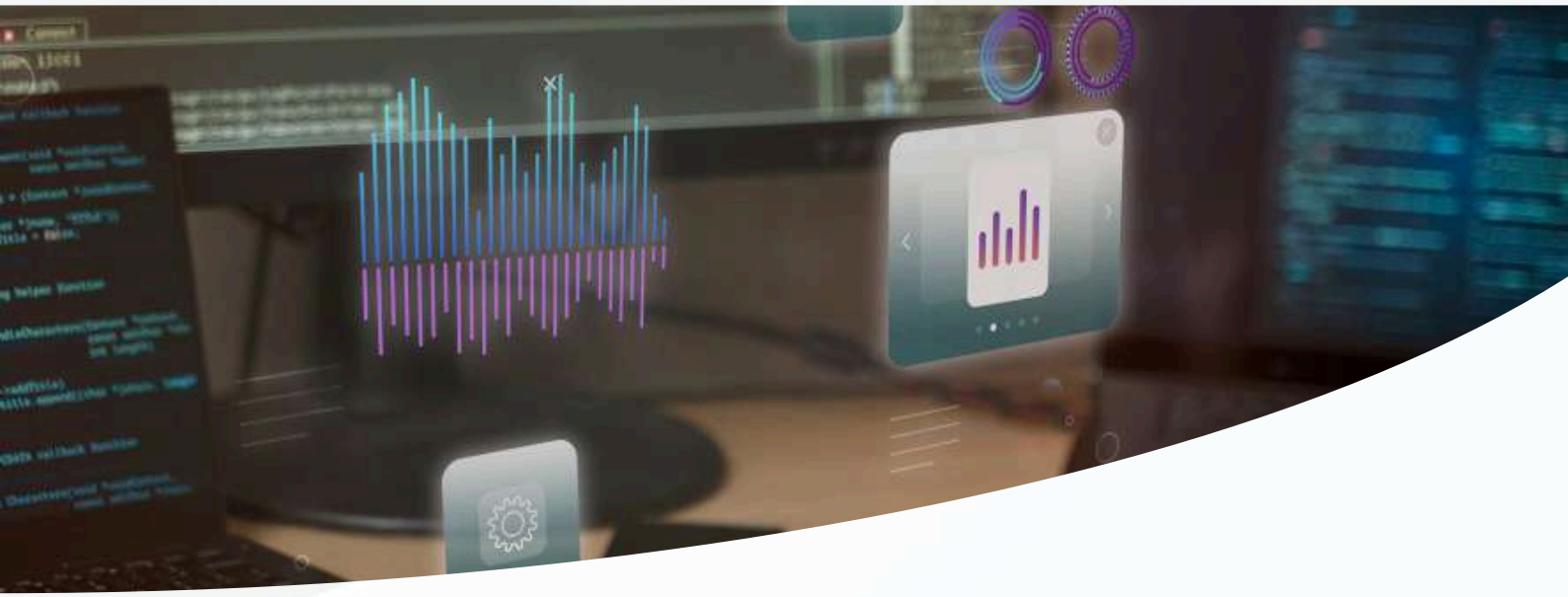
qualoom®

Inspiring Technology
for People

Introducción.
La transformación hacia DevSecOps en 2026

La evolución de DevOps hacia DevSecOps se ha acelerado debido a la creciente necesidad de **incorporar seguridad en todas las fases del ciclo de vida del software.** Las empresas enfrentan desafíos crecientes: amenazas sofisticadas, regulaciones más estrictas y la presión por acelerar la entrega de productos.

Este documento presenta un **Modelo de Madurez DevSecOps actualizado para 2026**, que permite a las organizaciones evaluar su capacidad de **integrar seguridad de manera efectiva** en pipelines de desarrollo y entrega continua.



qualoom®

Inspiring Technology
for People

Fundamentos de DevSecOps

En un entorno DevSecOps, la **seguridad deja de ser un proceso aislado** y se integra de manera nativa en todas las fases del ciclo de vida del software. Este enfoque combina **automatización, cultura organizacional y monitoreo continuo** para reducir riesgos y acelerar la entrega de software seguro.

Integración continua de la seguridad

01 Las pruebas de seguridad se incorporan directamente en los pipelines de CI/CD, incluyendo análisis de **SAST, DAST y análisis de composición de software (SCA).**

La automatización permite **detectar vulnerabilidades y desviaciones** de políticas en tiempo real, evitando que errores lleguen a producción. **02**

03 Se establece una **retroalimentación inmediata a los desarrolladores,** fomentando la corrección temprana y la mejora continua de la seguridad del código.

Seguridad como código (Security as Code)

01 Políticas, controles y configuraciones de seguridad se definen de manera programática, almacenadas en repositorios versionados y aplicadas automáticamente durante el despliegue.

Esto garantiza consistencia, reproducibilidad y auditabilidad, eliminando errores manuales y permitiendo cumplimiento de normas como ISO 27001, SOC 2 o GDPR. **02**

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Fundamentos de DevSecOps

03 Incluye gestión automatizada de secretos, credenciales y configuraciones críticas, evitando exposición accidental

Cultura de responsabilidad compartida

01 La seguridad no es exclusiva del equipo de DevOps; todos los roles, desde desarrollo hasta operaciones y QA, son responsables de la seguridad del producto.

Se fomentan prácticas de codificación segura, revisiones de código y capacitación continua, generando conciencia sobre riesgos y vulnerabilidades. 02

03 Esta cultura permite implementar Zero Trust interno, donde cada componente y acceso se valida constantemente.

Monitoreo continuo y observabilidad

01 Se implementa una monitorización integral de aplicaciones, infraestructura y contenedores, recopilando logs, métricas y eventos de seguridad.

Los sistemas de alerta se basan en análisis de comportamiento y correlación de eventos, permitiendo la detección temprana de anomalías o actividades sospechosas. 02

03 La información recolectada se utiliza para mejorar procesos, ajustar controles y apoyar auditorías, garantizando una gestión proactiva de riesgos.

Más información www.qualoom.es

qualoom®

Inspiring Technology for People

Niveles de Madurez DevSecOps

Nivel	Características	Objetivos de Seguridad	Ejemplo de Práctica
1 – Inicial	Seguridad reactiva, mínima automatización	Reducir riesgos críticos inmediatos	Escaneo manual de vulnerabilidades
2 – Definido	Procesos básicos de seguridad integrados	Cumplimiento de estándares mínimos	Integración de SAST/DAST en CI/CD
3 – Gestionado	Automatización de pruebas y despliegues	Reducción de tiempo de respuesta a vulnerabilidades	Pruebas de seguridad automatizadas en cada build
4 – Optimizado	Seguridad proactiva y continua	Innovación segura, reducción de incidentes	Análisis de amenazas en tiempo real y retroalimentación a Dev
5 – Avanzado	Cultura consolidada, gobernanza integrada	Resiliencia empresarial, seguridad predictiva	IA para detección de riesgos y auditoría continua

qualoom®

Inspiring Technology
for People

Beneficios de adoptar un modelo de Madurez DevSecOps

Reducción de riesgos

La integración de seguridad en pipelines CI/CD permite detectar y corregir vulnerabilidades de forma temprana, evitando errores críticos en producción y aumentando la confiabilidad del software.

Aceleración del time-to-market

La automatización de pruebas y controles reduce los retrasos por revisiones manuales, permitiendo despliegues rápidos y seguros, sin comprometer calidad ni seguridad.

Capacitación insuficiente

Políticas y controles automatizados, junto con registros trazables, facilitan auditorías y aseguran el cumplimiento de estándares como ISO 27001, SOC 2 o GDPR.

Cultura de innovación segura:

Equipos proactivos, conscientes de la seguridad, que colaboran desde el desarrollo hasta operaciones, adoptando mejores prácticas y respondiendo a riesgos de manera anticipada.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Estrategias para Avanzar en Madurez

Para avanzar en la madurez DevSecOps, las organizaciones deben combinar evaluación objetiva, automatización, cultura de seguridad y herramientas de monitoreo en un enfoque integrado y medible.

Evaluación del nivel actual

Realizar auditorías estructuradas de procesos, métricas de seguridad y análisis de riesgos para identificar brechas en integración de seguridad, cobertura de pruebas y gobernanza.

Automatización de pruebas y despliegues

Realizar auditorías estructuradas de procesos, métricas de seguridad y análisis de riesgos para identificar brechas en integración de seguridad, cobertura de pruebas y gobernanza.

Formación y concienciación del equipo

Capacitar de manera continua a desarrolladores, operadores y personal de QA, promoviendo la responsabilidad compartida y la adopción de prácticas de codificación segura y mitigación de riesgos.

qualoom®

Inspiring Technology
for People

Estrategias para Avanzar en Madurez

Integración de herramientas de monitoreo y análisis continuo

Implementar plataformas de observabilidad, SIEM y métricas de seguridad automatizadas para detección temprana de vulnerabilidades y anomalías a lo largo de toda la cadena DevSecOps.

Roadmap de madurez

Definir hitos claros para progresar en niveles de madurez, estableciendo indicadores de éxito, seguimiento de resultados y retroalimentación continua para la mejora del modelo de seguridad.

qualoom®

Inspiring Technology
for People

Asegura el futuro de tu Desarrollo de Software

La adopción de DevSecOps ha dejado de ser una iniciativa opcional para convertirse en un **pilar estratégico de resiliencia, eficiencia operativa y competitividad**. En un contexto marcado por ciclos de desarrollo acelerados, entornos cloud-native y un incremento constante de amenazas, integrar la seguridad de forma continua y automatizada es esencial para proteger el negocio sin frenar la innovación.

El **Modelo de Madurez DevSecOps 2026** proporciona un marco estructurado y medible que permite a las organizaciones **evaluar su estado actual, identificar brechas críticas y definir una hoja de ruta clara** para evolucionar hacia prácticas más maduras, seguras y alineadas con los objetivos del negocio. Su aplicación facilita una toma de decisiones informada sobre procesos, herramientas y capacidades del equipo, asegurando una mejora continua y sostenible.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Comienza tu **evaluación de madurez DevSecOps**

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808