

# Innovación y seguridad con **DevSecOps**



## RESUMEN EJECUTIVO

Ayudamos a una empresa destacada del sector asegurador a modernizar sus procesos de desarrollo de aplicaciones mediante la adopción de prácticas de DevSecOps. Con nuestro apoyo, integró herramientas y políticas que fortalecieron la seguridad, mejoraron la calidad del código y optimizaron los tiempos de entrega, impulsando la innovación continua en sus operaciones.

## EL RETO

La organización buscaba transformar su proceso de desarrollo para mantener su ventaja competitiva en un mercado dinámico.

Sin embargo, se enfrentaba a varios desafíos:

- Necesitaba puntos de validación en el desarrollo que redujeran tiempos, elevaran la calidad y garantizaran la seguridad.
- Era crucial implementar un esquema de seguridad a la medida, compatible con su cultura ágil y que asegurara el cumplimiento normativo.
- Además, requerían herramientas eficientes para identificar vulnerabilidades y optimizar el flujo de integración continua.

## LA SOLUCIÓN

IPCom diseñó e implementó una solución integral, trabajando de cerca con los equipos de la empresa para asegurar una adopción exitosa de DevSecOps. Las acciones incluyeron:

**Integración de herramientas SAST:** Permitiendo análisis de seguridad en tiempo real dentro del ciclo de desarrollo.

**Diseño de políticas personalizadas:** Creación de estándares de seguridad y calidad ajustados a las necesidades de la organización, con notificaciones automáticas para alertar a los equipos de desarrollo.

**Capacitación técnica:** Un acompañamiento continuo para asegurar el uso adecuado y la administración eficiente de las herramientas implementadas.

**Enfoque interdisciplinario:** IPCom aprovechó su experiencia técnica para coordinar con múltiples áreas del negocio, asegurando una solución que cumpliera objetivos operativos y estratégicos.

## RESULTADOS CLAVE

La implementación de DevSecOps generó mejoras significativas en los procesos de desarrollo de la organización:

### **Cobertura de seguridad ampliada:**

Las herramientas integradas en el ciclo de desarrollo permitieron detectar vulnerabilidades tanto en el código como en las aplicaciones, incluso después de ser implementadas. Esto fortaleció la confianza en la calidad de los entregables y redujo el riesgo de ataques cibernéticos.

### **Detección temprana de problemas:**

Vulnerabilidades críticas, como configuraciones inseguras o errores en el código, son detectadas en fases iniciales, evitando complicaciones y costos asociados a errores tardíos.

**Ahorro de tiempo y recursos:** Al automatizar pruebas de seguridad que antes eran manuales, lograron reducir los tiempos de validación en un 40%. Esto permitió a los equipos enfocarse en tareas más estratégicas, como la innovación y el desarrollo de nuevas funcionalidades.

### **Automatización eficiente:**

Al automatizar las pruebas de seguridad, el tiempo de validación se redujo drásticamente, pasando de días a horas en algunos casos. Además, los equipos pudieron dedicar más tiempo a actividades estratégicas, incrementando la productividad general.

### **Mejor calidad de código:**

Las políticas implementadas ayudaron a identificar problemas de código como duplicidades, complejidad excesiva y vulnerabilidades estructurales. Su pronta corrección mejoró la estabilidad, la funcionalidad y el rendimiento de las aplicaciones, asegurando experiencias de usuario más confiables.

**Email:** [contacto@ipcom.com.mx](mailto:contacto@ipcom.com.mx)

**Teléfono:** 55-5243-8633

**Ubicación:** María No. 200, Col. Nativitas, CP. 03500, CDMX.

*"El soporte de IPCom fue clave para integrar seguridad y calidad en nuestro ciclo de desarrollo, permitiéndonos innovar de forma ágil y segura."*