Introdución a DevOps/DevSecOps

Índice

Introdución

DevOps xurdiu a finais dos anos 2000 como unha resposta aos conflitos frecuentes entre desenvolvedores e administradores de sistemas:

- **Desenvolvedores** → Buscan entregar rápido, desenvolver novas funcionalidades, etc.
- **Administradores de sistemas** → Priorizan estabilidade, seguridade e control.

O termo foi popularizado por **Patrick Debois** en 2008 durante unha conferencia.

Problemas comúns

- "Funciona no meu portátil, pero non no servidor."
- Ciclos de entrega longos (meses ou anos).
- Fallos frecuentes en despregues.
- Mala comunicación entre equipos.

Definición

DevOps é unha cultura e conxunto de prácticas que:

- Facilita a colaboración entre **Desenvolvemento (Dev)** e **Operacións (Ops)**.
- **Automatiza** o ciclo de vida do software.
- **Acelera** o tempo de posta en produción sen comprometer a calidade.

Obxectivos

- **Integración continua (CI):** combinar cambios frecuentemente para detectar erros cedo.
- **Entrega continua (CD):** automatizar o despregue en ambientes de produción.
- **Monitorización e feedback continuo:** mellora baseada en datos reais.
- **Infraestrutura como código (IaC):** xestionar a configuración de forma automatizada e reproducible.

Tecnoloxías clave

Área	Tecnoloxías destacadas
Control de versións	Git, GitHub, GitLab
Integración continua	Jenkins, GitHub Actions, GitLab CI/CD
Contedores	Docker, Podman
Orquestración	Kubernetes, Docker Swarm
IaC	Ansible, Terraform, Helm
Monitorización	Prometheus, Grafana, ELK Stack

DevSecOps

Definición

Engade a **seguridade como responsabilidade compartida** durante todo o ciclo de vida do software.

Obxectivos

- Integrar seguridade dende o deseño.
- Automatizar a análise de vulnerabilidades.
- Evitar dependencias inseguras.
- Cumprir normativas sen frear a innovación.

DevSecOps – Medidas recomendadas por etapas

Etapa	Acción
Planificación	Análise de ameazas e requisitos de seguridade.
Desenvolvemento	Probas de software, análise estática.
Integración continua	Test de seguridade automatizados
Contedores	Escaneo de imaxes, uso de imaxes mínimas e firmadas.
Despregamento	Entornos illados, políticas de acceso.
Monitorización	Detección de intrusións en tempo real

Particularidades

- **Cambio de mentalidade** → A seguridade é responsabilidade de todos.
- **Automatización da seguridade:**
  - **SAST** (análise de código fonte): *SonarQube, Semgrep*
  - **DAST** (análise en execución): *OWASP ZAP*
  - **Análise de dependencias** (verificación de bibliotecas de terceiros): *Dependabot, Snyk*
- **Control de acceso baseado en roles.**
- **Conformidade e auditoría:** facilita cumprir normativas (ISO 27001, RGPD, NIST, HIPAA, etc.).

- A documentación automatizada facilita auditorías.

Vantaxes

- Redución de vulnerabilidades.
- Menor tempo de reacción ante incidentes.
- Maior confianza nos despregues.
- Adaptación a normativas sen frear a entrega.

Desafíos

- Cambio cultural dentro da organización.
- Curva de aprendizaxe das ferramentas.
- Exceso de alertas se non se configuran ben os sistemas de análise.

Recursos complementarios

- **What is DevSecOps? – Red Hat:**
  https://www.redhat.com/en/topics/devops/what-is-devsecops
- **OWASP DevSecOps Maturity Model:**
  https://owasp.org/www-project-devsecops-maturity-model/
- **Libros recomendados:**
  The Phoenix Project e *The DevOps Handbook*
- **Proxectos para probar:**
  Vulnerable Docker apps (DVWA, Juice Shop)
  https://hub.docker.com/r/vulnerables/web-dvwa