Lectura 3: 12-Factor App

- Son Principios de diseño y operaciones para realizar aplicaciones escalables.
- Entrega continua, contenedores y orquestadores
- Separar etapas build/release/run
- Shift-left (SAST, SCA): implementar seguridad, testeo desde etapas tempranas del desarrollo:
  - * SAST: structured analysis and design technique
  - * SCA: software composition analysis

Ahora veremos los 12 factores y su relacion con DevSecOps.

1) Codebase = Un solo repositorio por aplicación

Cada aplicación tiene una única base de código versionada

1 microservicio → 1 repositorio

2) Dependencias = Dependencias explícitas

Todas las dependencias se declaran explicitamente y versionada. (requirements.txt)

Enfoque DevSecOps SCA (escaneo de dependencias)

3) Config = Configuracion de variables de entorno

No se embebe en el codigo, se inyecta por variables de entorno

Variables de entorno : valores que un usuario define para el comportamiento de los procesos en ejecución

4) Backing Service = Servicios como recursos adjuntos

Se refiere a bases de datos, colas, caches o almacenamiento

TLS : Tranport Layer Security para conexiones o autenticación

5) Build, Release, Run = Etapas separadas

Built : empaqueta el artefacto

Release : Combina artefacto + configuracion / Versionado

Run : ejecuta la release en la plataforma

6) Processes = Aplicaciones stateless

Los procesos de la App no almacenan estado localmente, el estado va a servicios duraderos

Tip : evitar sesiones en memoria, diseñar idempotencia en operaciones

Enfoque DevSecOps : Reducir superficie de ataque

7) Port binding = servicios autocontenidos

La aplicacion expone su puerto (8080) y no depende de app server externos

8) Concurrency = Escalamiento horizontal

Escalar multiples instancias en paralelo

9) Disposability = Arranque y apagado rápido (graceful)

La app debe iniciarse y apagarse rapido, cerrando conexiones y liberando recursos

10) Dev / Prod parity = Paridad entre entornos

Mantener mínimas diferencias entre Dev, Staging y Prod: con la misma imagen deben cambiar solo los valores de configuración

OPA: Open Policy Agent, políticas de código abierto para lo nube nativa, que permite definir y aplicar políticas de seguridad en un sistema distribuido.

11) Logs = Flujos de eventos

La app escribe logs en STDOUT/STDERR, la plataforma los recolecta y enruta.

Enfoque DevSecOps: protección contra manipulación, detección contra comportamientos anómalos, alertas de seguridad y conservación para forensics

12) Admin Processes = Tareas puntuales

Los procesos administrativos se ejecutan con jobs o etapas del pipeline

RBAC: Rol-Based Access Control, busca mínimos privilegios, auditorías detalladas, controles con expiración

Resumen de factores:

1 → Pipeline CI/CD

2-5 → Contenedores

6-9 → Kubernetes

10 → Paridad

11-12 → Observabilidad y auditoría