

1. La seguridad como diseño (Las 4 Cs): En kubernetes la seguridad es importante y se basa en el modelo de las 4Cs: Cloud, Cluster, Container, Code, un fallo compromete el sistema

2. RBAC: Identidad y minimo privilegio "control de acceso basado en roles"

↓ Se define como **quien** puede hacer **qué** sobre **qué** (recurso)

* Usar tokens de vida corta

3. Policies y Admission Control: La "aduanas".

Antes que el recurso se cree, debe pasar por los Admission Controllers:

- Pod security standards: Perfiles nativos
- ValidatingAdmissionPolicy: reglas nativas
- Externos: OPA Gatekeeper

4. NetworkPolicies: Hacia el Zero-Trust: En kubernetes todos los pods se ven entre si, eso es peligroso, se debe aplicar:

* NetworkPolicies para segmentar trafico

* Patrón de oro: bloquear todo en el namespace y luego abrir solo los puertos necesarios

5. Integración en el Pipeline:

* Definir namespace y Roles en los pipelines

* CI (Build): escaneo de imagenes y validacion (linters).