KubeBackup360

Inter Tight

Sistema Automatizado de Resiliencia y Recuperación en Entornos Kubernetes

---

Proyecto Final ASIR | Institut Puig Castellar
Curso 2025-2026

Luis Alfredo Florez
(Infraestructura y Core)

Clara Inés Nchama
(Documentación y Monitorización)

Ilias Brahimi
(Red y Pruebas)

La fragilidad de los sistemas distribuidos modernos

En infraestructuras modernas basadas en contenedores, la naturaleza efímera de los Pods choca con la necesidad de persistencia de datos. Los errores de configuración, el 'drift' y los fallos de nodo son inevitables.

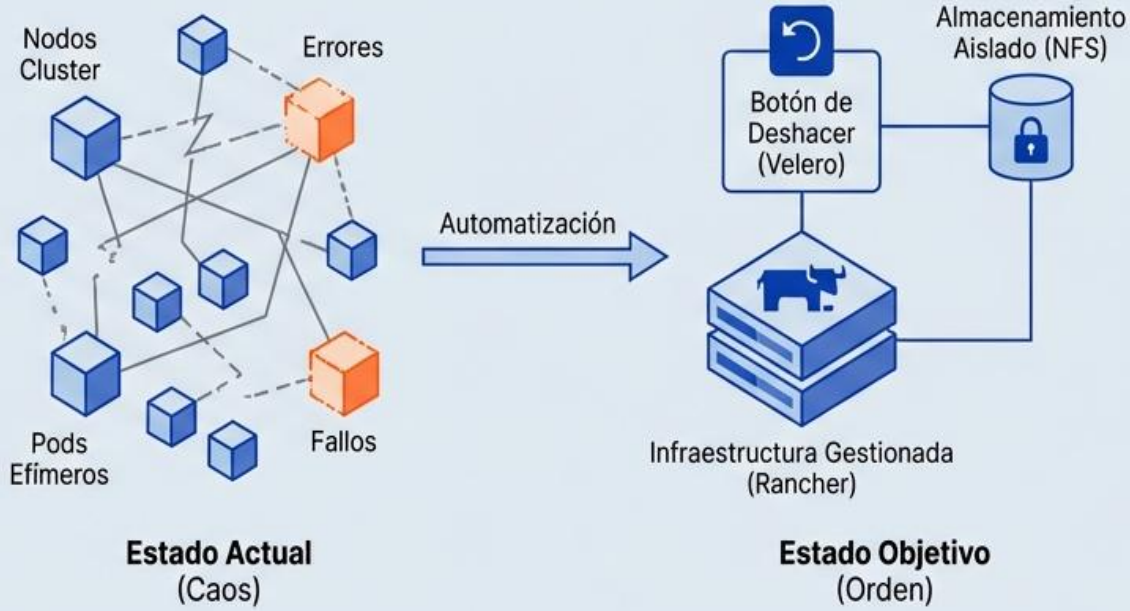
⚠ El Problema

Falta de mecanismos centralizados.

En entornos educativos y de laboratorio, la estrategia de recuperación ante desastres (DRP) suele ignorarse, dejando los datos vulnerables.

La Solución: KubeBackup360

Una infraestructura Kubernetes gestionada (Rancher) que integra un "botón de deshacer" automatizado (Velero) y almacenamiento aislado (NFS).

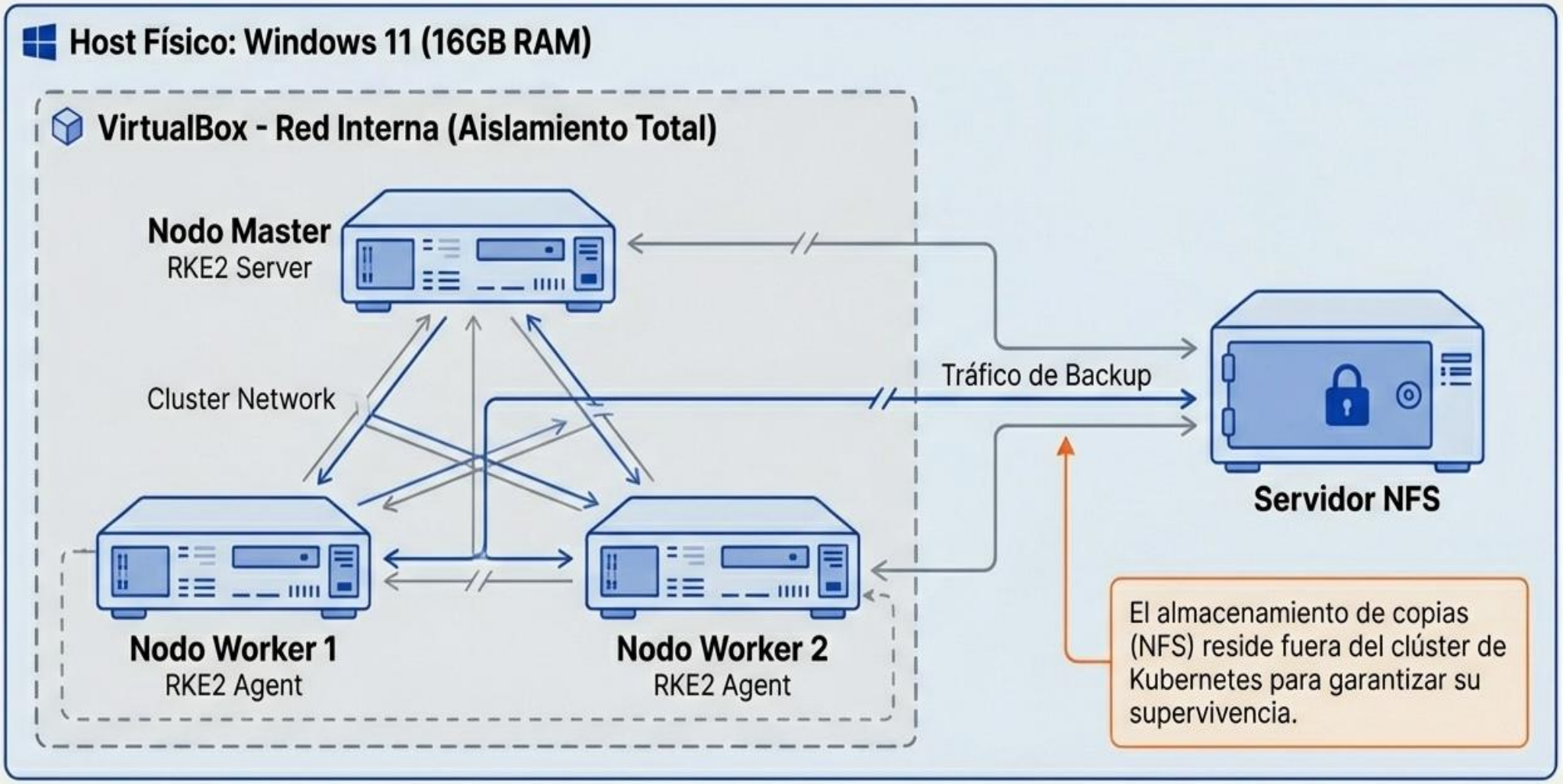


Estado Actual
(Caos)

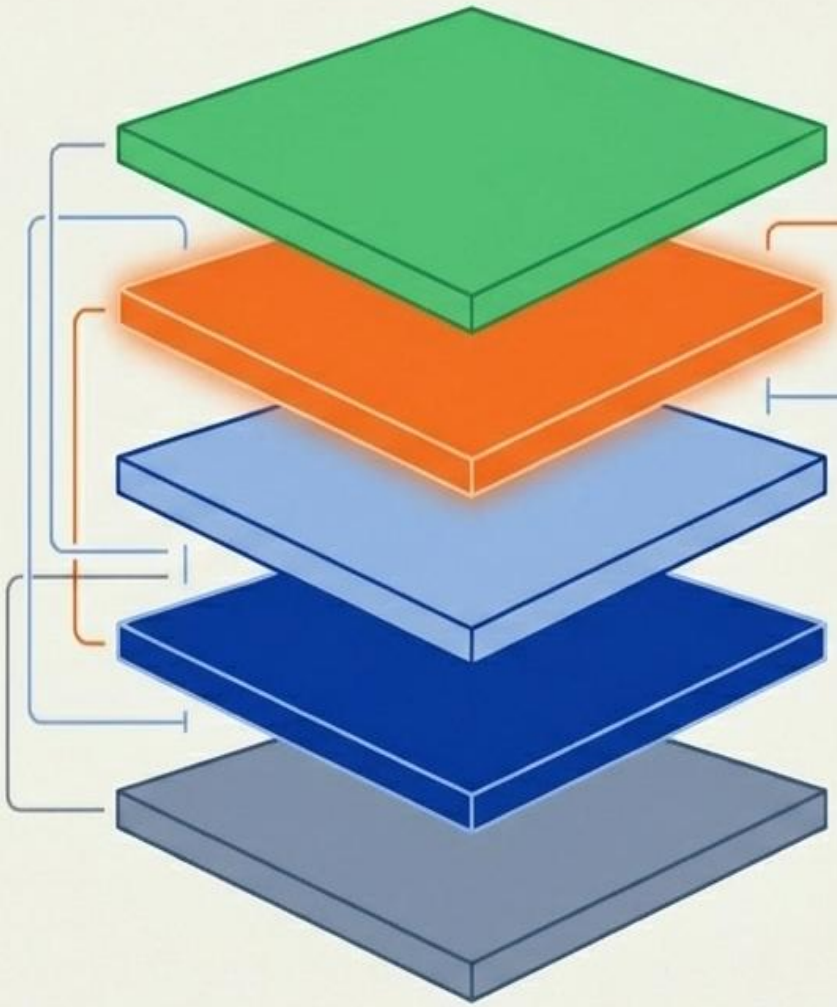
Estado Objetivo
(Orden)

Objetivo: Diseñar, desplegar y validar una estrategia de recuperación capaz de restaurar servicios tras un fallo catastrófico. →

Topología de red y aislamiento del entorno



Stack tecnológico: Capas de ingeniería



Capa 5: Observabilidad
Prometheus + Grafana. Métricas de salud y validación de restores.

Capa 4: Protección
Velero + NFS + Restic. El motor de snapshots y la bóveda de almacenamiento.

Capa 3: Gestión
SUSE Rancher + Helm. Gestión visual centralizada y despliegue de paquetes.

Capa 2: Orquestación
Kubernetes RKE2. Certificada CNCF, segura por defecto (CIS Benchmarks) y ligera.

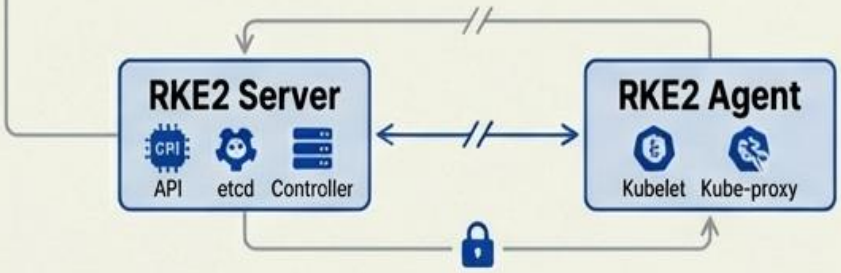
Capa 1: Infraestructura Base
VirtualBox + Ubuntu Server 24.04 LTS. Estabilidad y bajo consumo (headless).

El motor de orquestación: RKE2 y Seguridad

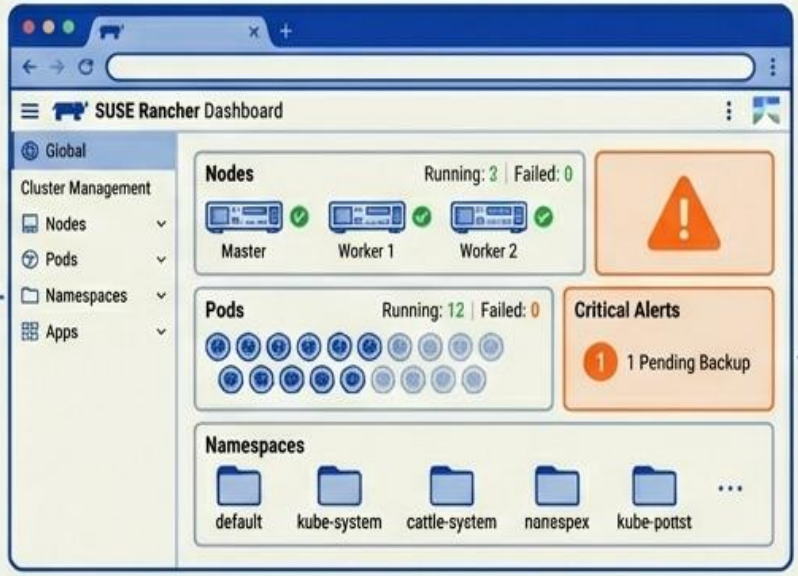
RKE2 (K3s para el Datacenter)

RKE2

- **Ventaja Técnica:** Binario optimizado que incluye API Server, etcd y controller-manager.
- **Seguridad:** Cumplimiento FIPS y configuración pre-endurecida sin intervención manual.

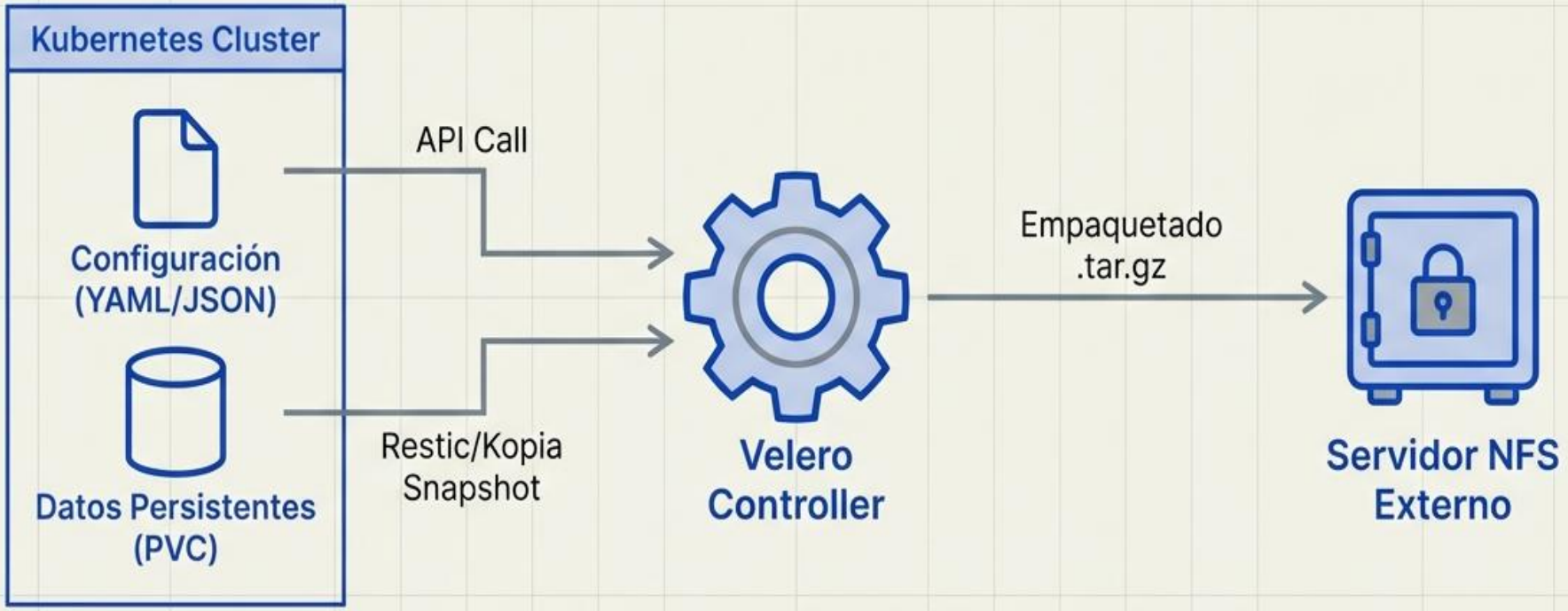


SUSE Rancher (Panel Unificado)



- **Función:** Abstracción visual de la complejidad de kubectl.
- **Valor:** Visualización inmediata de Nodos, Pods y Namespaces para administración eficiente.

Inter Tight
Mecánica de protección: Anatomía de un Backup




```
velero schedule create daily-backup --schedule='0 3 * * *' --ttl 72h
```

Automatización mediante CRDs para políticas recurrentes.

Ciclo de vida del dato: De la imagen a la persistencia

1. Construcción

Dockerfile → Imagen (NGINX/MariaDB) → Docker Hub.

2. Despliegue

Manifiestos YAML definen StatefulSets y Deployments.

3. Persistencia

Solicitud de PVC vinculada a un Persistent Volume (PV).

Insight Crítico

Los Pods son mortales; los datos en los PVCs deben ser inmortales. KubeBackup360 desacopla el dato del contenedor.

La Bóveda de Seguridad: Estrategia NFS

Implementación Técnica
nfs-kernel-server en Linux independiente.
Montaje estándar en nodos.

Control de Acceso
Exportación restringida por IP y permisos de red internos.

Principio de Seguridad
Aislamiento de fallos. El backup reside fuera del "Blast Radius" del clúster.

NFS Server (Linux)

Adaptación 3-2-1

Escenarios de recuperación y validación (DRP)

Scenario A: The Oops

Borrado accidental de Namespace.

Result:
Restauración granular de recursos por etiqueta.

Scenario B: The Crash

Fallo de nodo o corrupción de datos.

Result:
"Full Restore" de PVCs a un punto en el tiempo.

Scenario C: State Drift

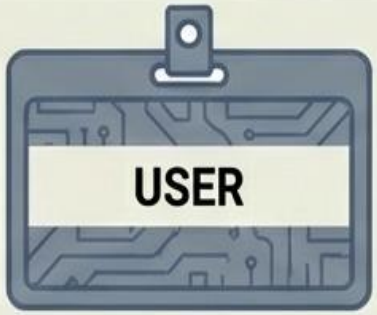
Configuraciones alteradas manualmente.

Result:
Restauración del "estado deseado" desde YAML.

Gobernanza y Seguridad: RBAC y Cifrado

RBAC (Role-Based Access Control)

- Deploy, Backup, Restore, Destroy.



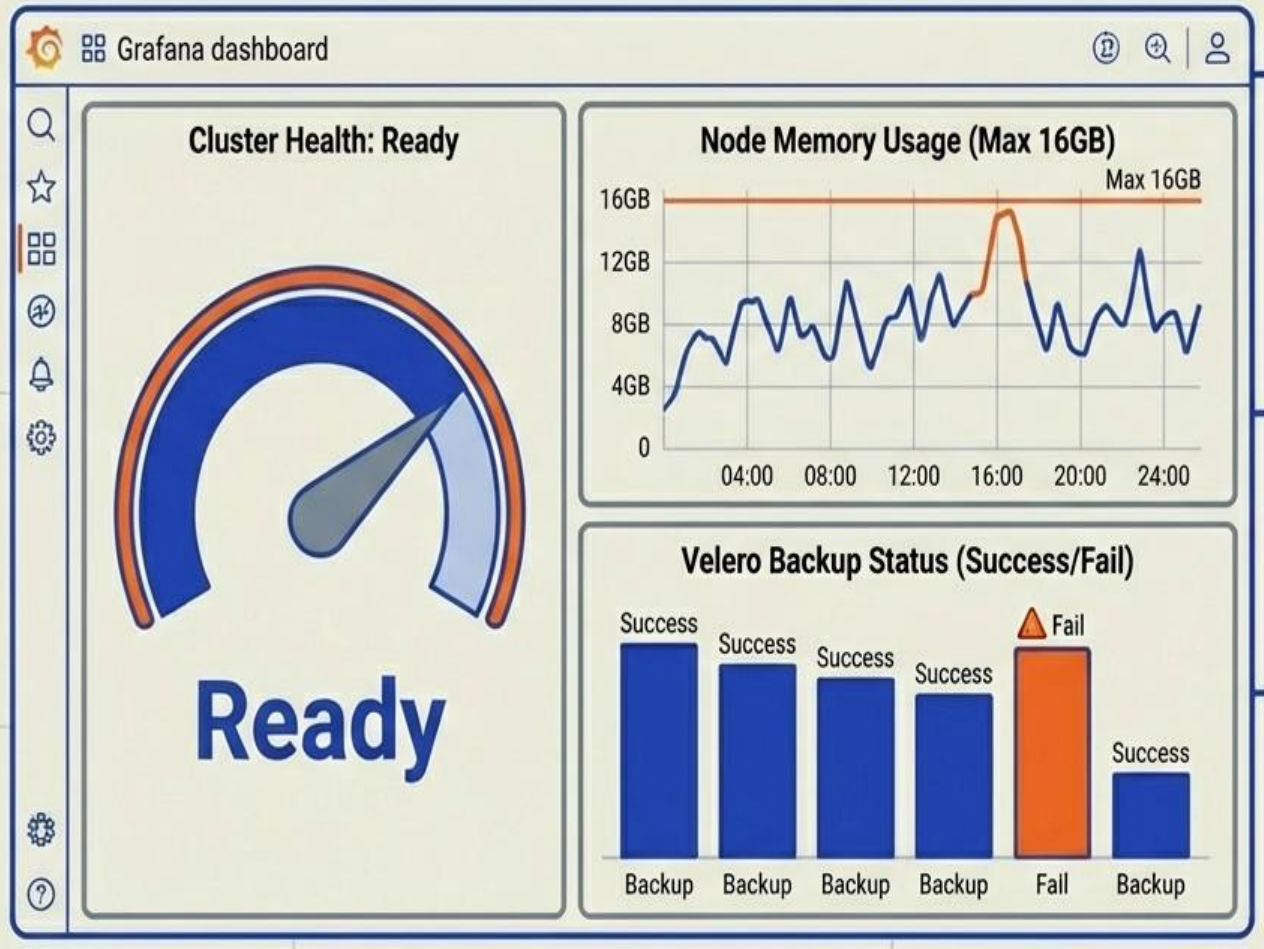
- Read-only, View Dashboards.

Protección de Datos

Uso de GPG/OpenSSL para cifrar los archivos de backup en reposo.

Network Policies: Aislamiento lógico entre namespaces para evitar movimientos laterales.

Observabilidad: Monitorización de salud



Prometheus:
Recolecta métricas (scraping) de nodos y pods.

Grafana:
Visualiza el pulso del sistema.

Validación:
Confirmación visual de estabilidad pre y post-restore.

Roadmap de ejecución: Fases del proyecto

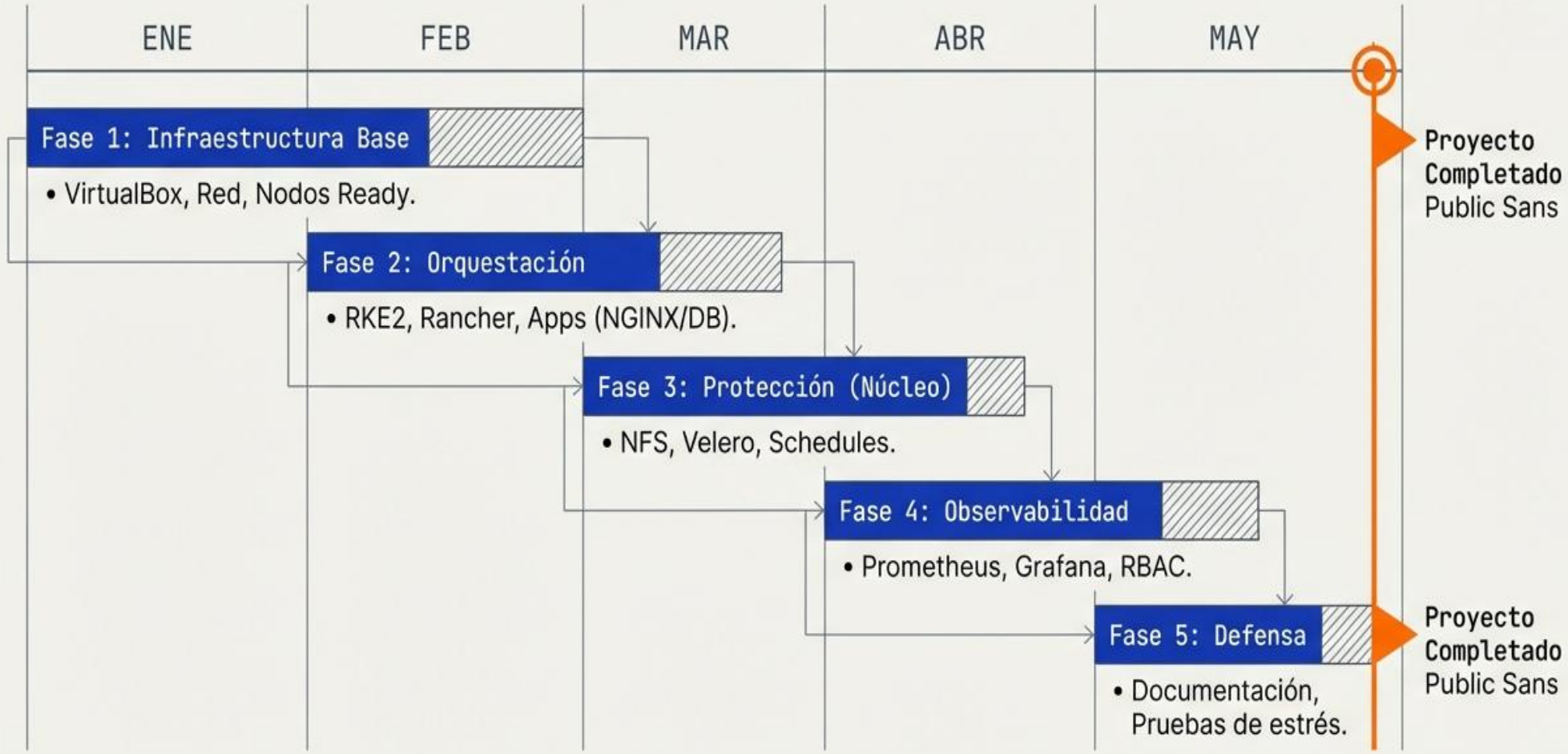
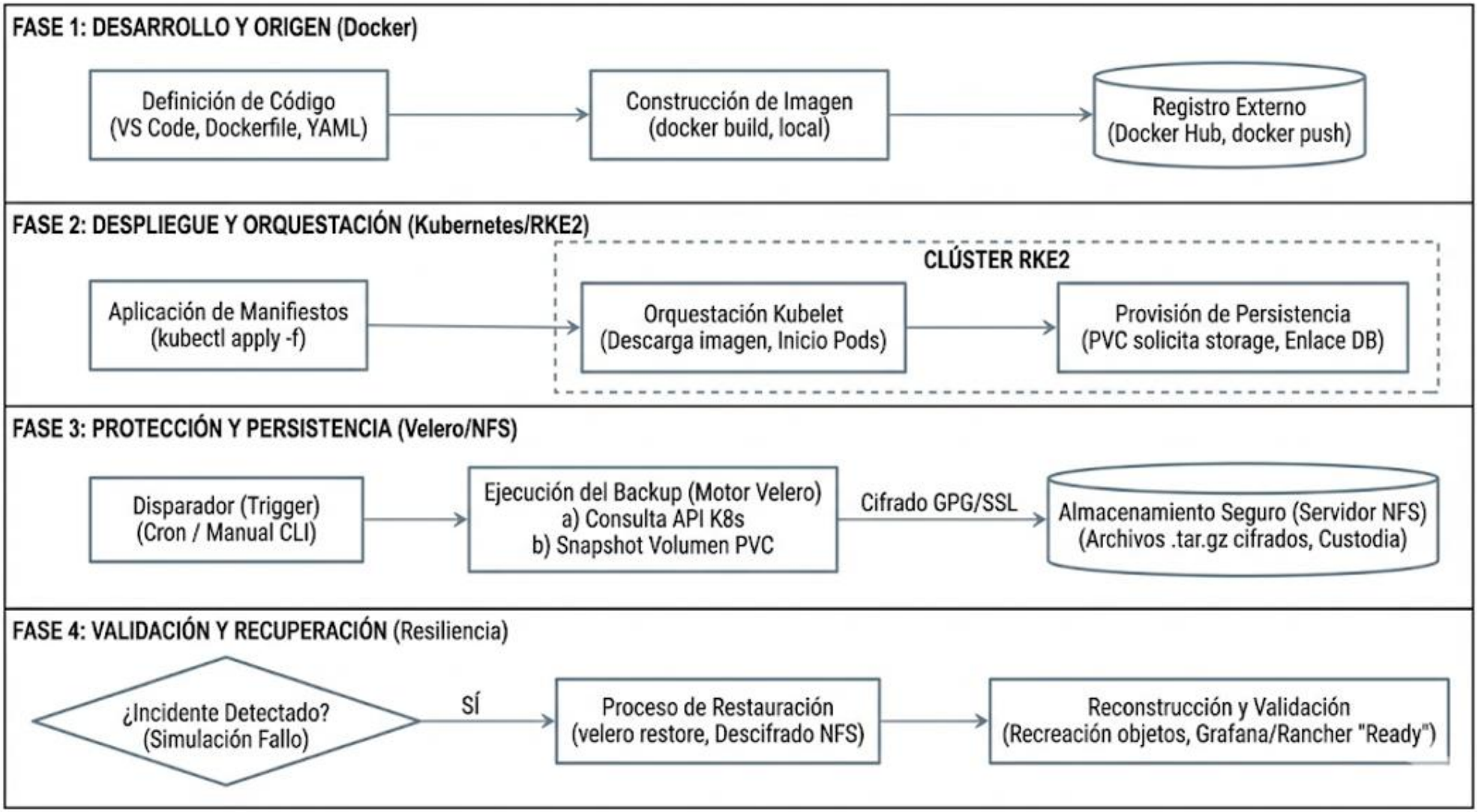


Diagrama de flujo del ciclo de vida operativo y de resiliencia del sistema KubeBackup360.



Análisis de riesgos y mitigación

Hardware

Riesgo: 16GB RAM Límite.

Mitigación: RKE2 ligero + Ubuntu Server headless.

Consistency

Riesgo: Entornos diversos.

Mitigación: IaC y repositorio Git centralizado.

Inter Tight

Data

Riesgo: Backup corrupto.

Mitigación: Tests de integridad y “Fire Drills”.

External

Riesgo: Docker Hub down.

Mitigación: Caché local de imágenes.

9. Flujo de Validación y Criterios de Éxito KubeBackup360

9.1 CRITERIOS DE ACEPTACIÓN
(CONDICIONES NECESARIAS)

- ✓ Clúster y nodos operativos.
- ✓ Despliegue de servicios (NGINX).
- ✓ Funcionalidad de Backup exitosa.
- ✓ Restauración tras fallo simulado.
- ✓ Gestión vía Rancher y CLI.
- ✓ RBAC básico (Admin vs Limitado).
- ✓ Reproducible en laboratorio.

→

9.2 PRUEBAS PREVISTAS
(VERIFICACIÓN DEL CUMPLIMIENTO)

🛠️ Pruebas Funcionales

- ✓ Verificación estado clúster.
- ✓ Ejecución manual de backups (Velero).
- ✓ Restauración tras eliminación de recursos.
- ✓ Comprobación de persistencia de datos.

👤 Pruebas de Usuario

- ✓ Acceso administrador (Rancher).
- ✓ Verificación de restricciones RBAC.
- ✓ Uso de CLI para administración.

📈 Rendimiento y Estabilidad

- ✓ Revisión métricas básicas (CPU/RAM).
- ✓ Estabilidad post-backup/restore.

→

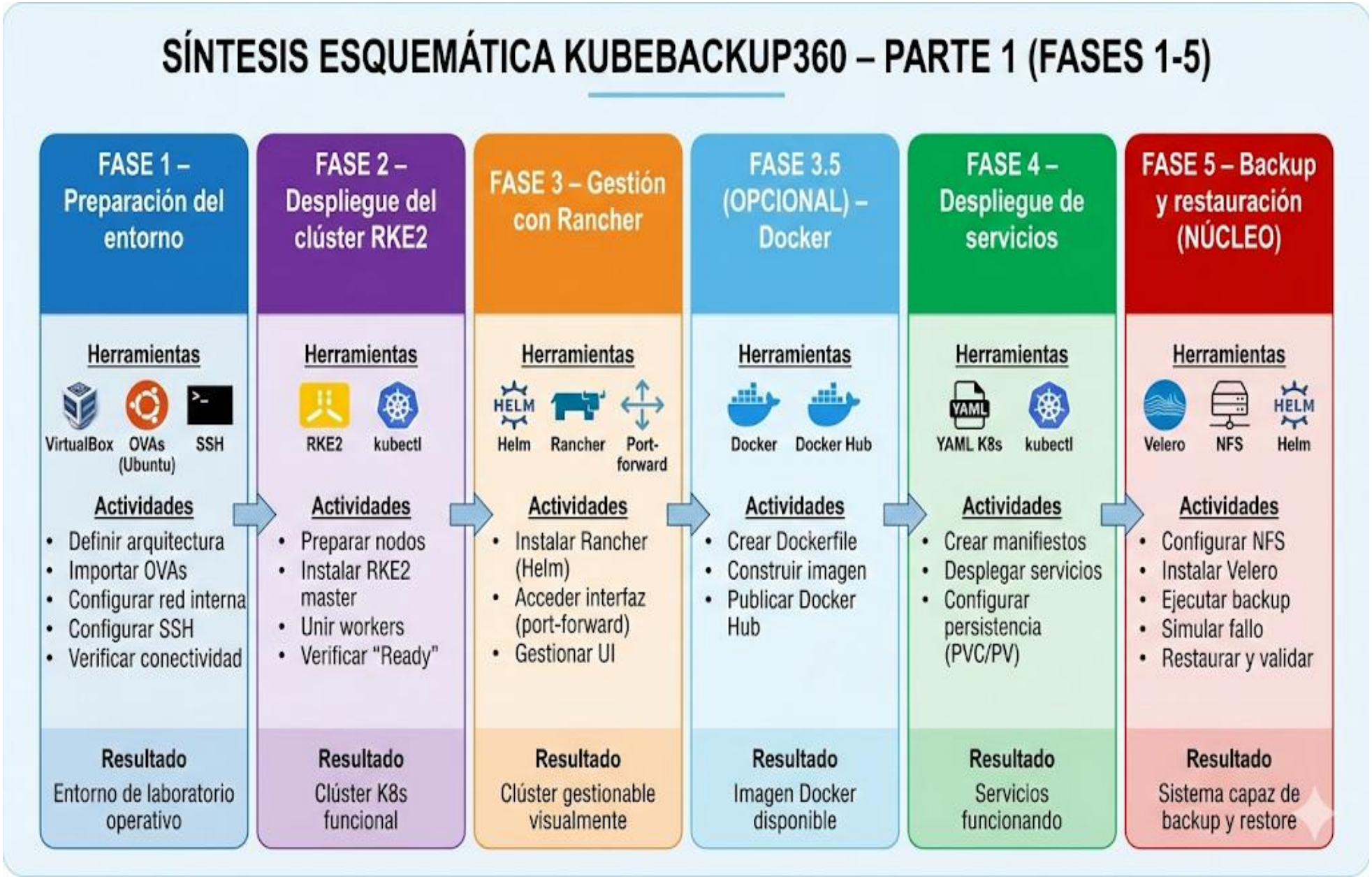
9.3 INDICADORES DE CALIDAD
(RESULTADOS ESPERADOS)

- ✓ Clúster operativo tras fallos.
- ✓ Servicios restaurados correctamente desde backup.
- ✓ Ausencia de errores críticos post-restauración.
- ✓ Métricas estables en monitorización.
- ✓ Sistema documentado y reproducible.

Criterios de éxito y validación final

- **Infraestructura:** Clúster RKE2 estable y operativo.
- **Servicios:** NGINX y MariaDB desplegados con persistencia.
- **Protección:** Backups automatizados hacia NFS sin errores.
- **Resiliencia:** Restauración exitosa tras borrado intencionado (RTO funcional).
- **Gestión:** Administración vía Rancher y RBAC validado.

SÍNTESIS ESQUEMÁTICA KUBEBACKUP360 – PARTE 1 (FASES 1-5)



VISIÓN GENERAL: EL PROBLEMA Y LA SOLUCIÓN

**El Problema: ** La adopción de Kubernetes es el estándar actual.

Pero su naturaleza distribuida y efímera hace que la gestión de la persistencia de datos y la recuperación ante desastres sea compleja.

Un clúster sin una estrategia de backup probada, “es un riesgo inaceptable en un entorno empresarial.”

**La Solución: “”KubeBackup360“” **

No es solo un clúster para desplegar aplicaciones. Es un proyecto de ingeniería de sistemas enfocado en la **resiliencia**.

Construiremos un entorno tipo laboratorio que simula producción para implementar, validar y documentar una estrategia completa de Disaster Recovery (DRP) utilizando herramientas estándar del sector como Velero, asegurando que podemos recuperar el servicio completo tras un fallo catastrófico.

SÍNTESIS ESQUEMÁTICA KUBEBACKUP360 - PARTE 2 (FASES 6-8)