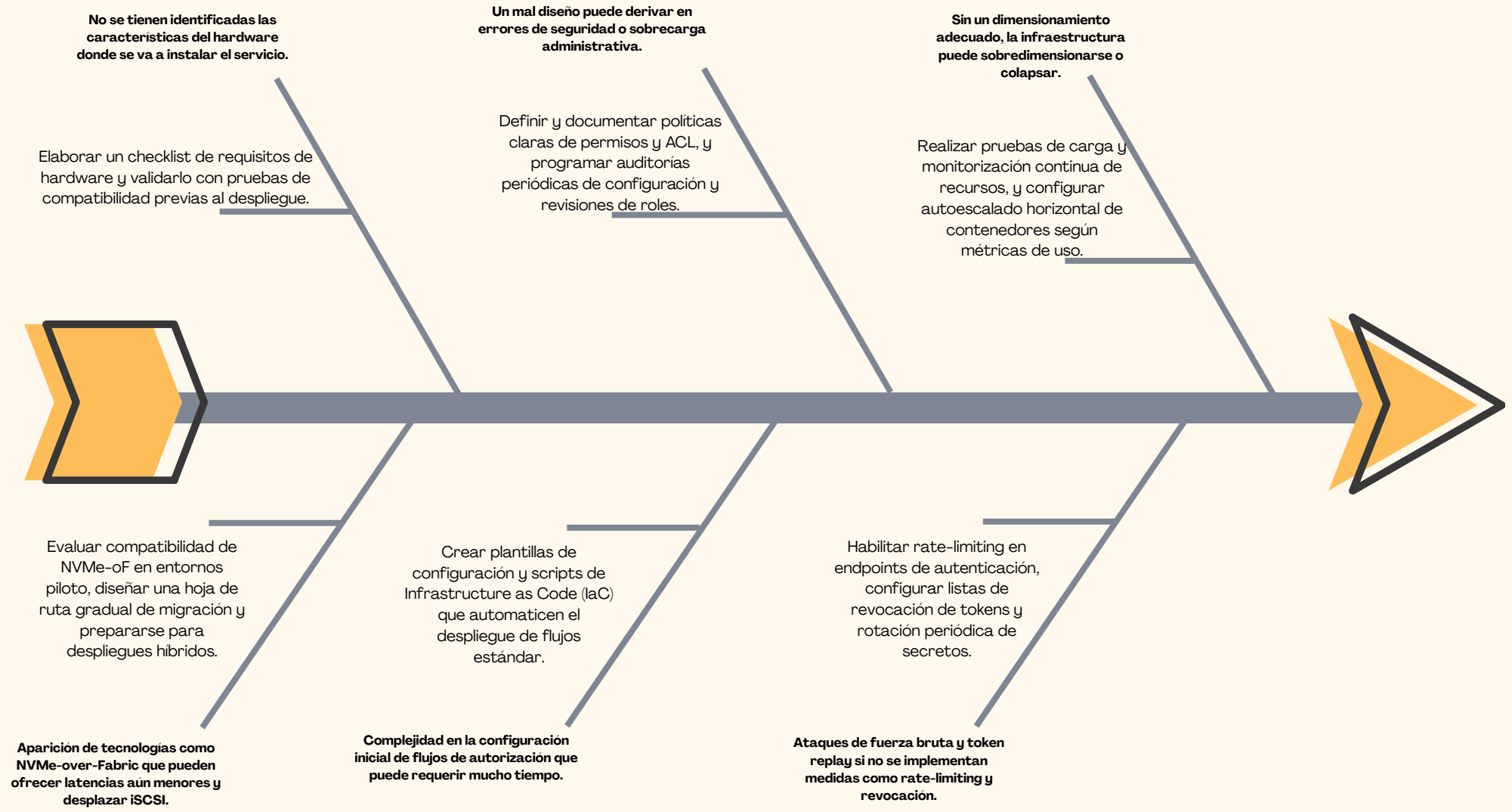
No se tienen identificadas las características del hardware donde se va a instalar el servicio.
Elaborar un checklist de requisitos de hardware y validarlo con pruebas de compatibilidad previas al despliegue.
Un mal diseño puede derivar en errores de seguridad o sobrecarga administrativa.
Definir y documentar políticas claras de permisos y ACL, y programar auditorías periódicas de configuración y revisiones de roles.
Sin un dimensionamiento adecuado, la infraestructura puede sobredimensionarse o colapsar.
Realizar pruebas de carga y monitorización continua de recursos, y configurar autoescalado horizontal de contenedores según métricas de uso.
Evaluar compatibilidad de NVMe-oF en entornos piloto, diseñar una hoja de ruta gradual de migración y prepararse para despliegues híbridos.
Aparición de tecnologías como NVMe-over-Fabric que pueden ofrecer latencias aún menores y desplazar iSCSI.
Crear plantillas de configuración y scripts de Infrastructure as Code (IaC) que automaticen el despliegue de flujos estándar.
Complejidad en la configuración inicial de flujos de autorización que puede requerir mucho tiempo.
Habilitar rate-limiting en endpoints de autenticación, configurar listas de revocación de tokens y rotación periódica de secretos.
Ataques de fuerza bruta y token replay si no se implementan medidas como rate-limiting y revocación.


Accesos mal configurados pueden exponer información crítica.
Revisar y ajustar permisos regularmente y aplicar el principio de menor privilegio en todas las cuentas de servicio.
Empleados con privilegios excesivos o mal gestionados.
Definir políticas claras de roles y separación de funciones, y llevar a cabo auditorías periódicas de privilegios.
Curva de aprendizaje elevada para la administración de iSCSI que exige conocimientos especializados.
Desarrollar un plan de formación interna con guías paso a paso y laboratorios prácticos de administración iSCSI.
Incorporar mecanismos de análisis de comportamiento (machine learning) sobre los eventos recibidos para filtrar ruido.
Mejora la detección de anomalías y reduce falsos positivos.
Impartir formación continua en ciberseguridad, habilitar autenticación multifactor (MFA) y filtros anti-phishing en correo.
Phishing y robo de credenciales.
Implementar políticas de escalación automática, generar logs de auditoría de todas las alertas y establecer revisiones de bitácoras.
Alertas silenciadas o mal gestionadas internas difíciles de detectar; usuarios legítimos actuando maliciosamente.