Checklist de Implementación segura del aislamiento de red

1. Planificación de la segmentación

- ☑ Identificar activos críticos (servidores, bases de datos, aplicaciones)
- ☑ Clasificar zonas por nivel de confianza (interna, externa, DMZ)
- ☑ Definir políticas de comunicación entre zonas
- ☑ Documentar el diseño lógico y físico de la red

2. Configuración de aislamiento

- ☑ Crear VLANs según funciones o departamentos
- ☑ Configurar subredes con rangos IP separados
- ☑ Aplicar ACLs para controlar tráfico entre segmentos
- ☐ Definir reglas de firewall estrictas por zona

3. Aislamiento en entornos virtuales y cloud

- ☑ Configurar redes internas entre VMs y contenedores

- [x] Usar VPCs con subredes privadas y públicas separadas
- [ ] Aplicar Security Groups y NACLs en entornos cloud
- [x] Segmentar entornos de desarrollo, test y producción

4. Monitoreo y detección

- [x] Implementar SIEM para análisis de logs y correlación de eventos
- [x] Instalar IDS/IPS entre segmentos críticos
- [x] Configurar alertas de tráfico entre zonas no autorizadas
- [x] Habilitar logging de firewall y flujos de red (NetFlow, VPC Flow Logs)

5. Pruebas y validación

- [x] Realizar escaneos de red internos para verificar aislamiento
- [x] Comprobar accesibilidad entre zonas según las políticas
- [x] Simular intentos de acceso no autorizado para probar alertas
- [ ] Validar cumplimiento de normas (ISO 27001, NIST, PCI-DSS)

6. Gestión continua

- ☑ Revisar periódicamente las reglas de firewall y ACLs
- ☑ Actualizar el diagrama de red ante cambios
- ☐ Formar al personal en políticas de segmentación
- ☐ Auditar accesos y tráfico entre zonas sensibles

Resumen Ejecutivo

La implementación del aislamiento de red muestra un enfoque sólido en la segmentación por zonas de confianza, uso de VLANs, firewalling y control de acceso, tanto en entornos físicos como virtualizados y cloud. Se han aplicado medidas de monitoreo (SIEM, IDS/IPS, alertas) y validación mediante escaneos y pruebas de cumplimiento normativo, lo que refuerza la postura de seguridad general.

Sin embargo, se detectan aspectos a mejorar:

- Falta detalle sobre la documentación actualizada del diseño físico/lógico.
- No se especifican logs de pruebas de accesibilidad ni resultados de simulaciones de ataques.
- La gestión continua aún no contempla métricas de revisión ni evidencias de auditoría efectiva.
- No se menciona si el personal fue capacitado recientemente.

Conclusión: El aislamiento está bien diseñado e implementado, pero necesita reforzarse en documentación, validación práctica y seguimiento continuo para asegurar su eficacia a largo plazo.