Nº	Riesgo Arquitectónico	Categoría	Probabilidad	Impacto	Severidad
1	Dependencia de un único perfil técnico para la migración a Snowflake	Organizacional / Operativo	Media	Alta	Alta
2	Integración incompleta de Purview-Snowflake	Normativo / Seguridad	Media	Alta	Alta
3	Clasificación y retención no alineada entre Azure y Snowflake	Normativo	Media	Alta	Alta
4	Doble escritura genera errores de integridad	Técnico	Alta	Media	Alta
5	Vendor lock-in Azure + Snowflake	Técnico / Estratégico	Media	Media	Media
6	Sobrecostos en Snowflake por cargas analíticas	Financiero / Técnico	Alta	Media	Alta
7	Riesgos en ingestión desde fuentes externas	Operativo	Alta	Media	Alta
8	Exposición de APIs (Spoofing / Tampering / EoP)	Seguridad (STRIDE)	Media	Alta	Alta
9	Divulgación de información sin autorización	Seguridad / Normativo	Bajo	Alta	Media
10	DoS sobre APIs críticas	Seguridad	Media	Media	Media
11	Repudio de operaciones críticas	Seguridad	Bajo	Media	Baja
12	Exposición indirecta por uso de VPN para fuentes	Seguridad / Infraestructura	Media	Alta	Alta
13	Brecha de skill técnico para Snowflake	Organizacional	Alta	Media	Alta
14	Curva de aprendizaje del suplente técnico	Organizacional	Media	Media	Media
15	Costos adicionales por gobernanza / Firewalls / VNET	Financiero	Bajo	Medio	Baja

Controles Existentes	Mitigación Propuesta	Vista Impactada
Conocimiento parcial documentado	Suplente técnico, capacitación cruzada, documentación completa	Negocio / Aplicaciones
Purview configurado solo en Azure	Conector Purview–Snowflake, sincronización automática, validación auditada	Información / Seguridad
Políticas de retención en Azure	Configurar Time Travel, Fail-safe y políticas de retención unificadas	Información / Seguridad
Validaciones en backend	Reconciliación diaria, logs transaccionales, pruebas por dominio, rollback	Información / Aplicaciones
APIs estándar	Arquitectura API-first, contratos desacoplados, dominio de datos independiente	Aplicaciones / Infraestructura
Warehouses manuales	Auto-suspend/resume, optimización de consultas, governance de consumo	Infraestructura
Validaciones básicas en APIM	Rate limiting, transformaciones seguras, monitoreo, colas/reties	Aplicaciones
MFA, APIM, WAF, RBAC	Token hardening, Zero Trust, payload encryption	Seguridad / Aplicaciones
TLS 1.3, Private Endpoints, Defender for Cloud	Integración con SIEM, detección de anomalías	Seguridad / Datos
Front Door + WAF	Redundancia, rate limiting avanzado	Infraestructura
Auditoría en Azure	Firmas digitales, auditoría cruzada en Sentinel y Snowflake	Seguridad
VPN Gateway	Firewall corporativo, VNET dedicada, Private Endpoints, Zero Trust	Infraestructura
Conocimiento parcial del equipo	Capacitación formal, talleres, shadowing	Negocio / Datos
Documentación inicial	Checklist de migración, pairing, sesiones de transferencia de conocimiento	Negocio
Arquitectura actual	Modelos de costo previsibles, optimización de topologías	Infraestructura