INFORME TÉCNICO DE AUDITORÍA DE CIBERSEGURIDAD EN LA NUBE

Evaluación de Arquitectura Multicloud, Matriz de Vulnerabilidades y Brechas Normativas | Fuente: Oficina del CISO & IT Risk

1. RESUMEN EJECUTIVO Y ALCANCE

Durante el tercer trimestre de 2026, la firma auditora externa evaluó la postura de seguridad y cumplimiento normativo de la infraestructura en la nube (Microsoft Azure & AWS Enterprise) del Banco Nacional de Crédito. Se identificaron un total de **14 hallazgos**, de los cuales **3 son clasificados como Críticos** por su impacto potencial ante la próxima inspección regulatoria de la CNBV y el Banco Central.

2. MATRIZ DE HALLAZGOS CRÍTICOS Y CUMPLIMIENTO

ID	Vulnerabilidad / Brecha Detectada	Nivel de Riesgo	Norma Afectada	Impacto Regulatorio / Técnico
SEC-01	Configuración errónea de IAM con permisos excesivos en contenedores de datos (S3 / Azure Blob Storage)	**CRÍTICO**	CNBV Cap. IX / ISO 27001	Riesgo de fuga de datos de cuentahabientes y multa de hasta 50,000 UMA.
SEC-02	Falta de cifrado en tránsito en microservicios legacy de conexión Core-Bancario a Nube	**CRÍTICO**	PCI-DSS v4.0 / NIST 800-53	Intercepción de credenciales API y suspensión de certificación PCI.
SEC-03	Ausencia de autenticación multifactor (MFA) obligatoria en el 12% de las cuentas de desarrollo	**ALTO**	Politica Interna CISO-04	Vulnerabilidad ante ataques de ingeniería social y Phishing focalizado.
SEC-04	Retraso en la aplicación de parches de seguridad en clusters de Kubernetes (EKS)	**ALTO**	CIS Benchmarks v3.1	Exposición a exploits conocidos de elevación de privilegios.

3. PLAN DE REMEDIACIÓN Y COMPROMISO IT (30 DÍAS)

- **Remediación IAM (Hito SEC-01):** Implementación de políticas de Menor Privilegio (Least Privilege) y acceso JIT (Just-In-Time) automatizado por Entra ID. *Fecha compromiso: 20 de Septiembre.*
- **Cifrado de Comunicaciones (Hito SEC-02):** Despliegue de mTLS (Transport Layer Security Mutuo) en el Service Mesh para todas las conexiones Core-Nube. *Fecha compromiso: 30 de Septiembre.*
- **Enforcement de MFA (Hito SEC-03):** Bloqueo automático de acceso a la consola de administración a toda cuenta sin FIDO2/MFA habilitado. *Fecha compromiso: 15 de Septiembre.*