INFORME AUDITOR DE CIBERSEGURIDAD E INFRAESTRUCTURA CLOUD

Evaluación de Cumplimiento Normativo y Vulnerabilidades Previo a Auditoría Regulatoria | Ref: Security_Cloud_Audit.pdf

Página 1 | Sección 1.1: Marco Normativo y Alcance de la Auditoría

Se ejecutó una auditoría integral sobre la infraestructura multicloud del banco (AWS y Azure), evaluando el cumplimiento contra los estándares ISO/IEC 27001:2022, las Disposiciones de Ciberseguridad de la CNBV y PCI-DSS v4.0. El alcance abarcó los servicios de almacenamiento S3, gestión de identidades IAM y clústeres de contenedores AKS donde procesan las transacciones bancarias core.

Sección 2.3: Hallazgos Críticos de Seguridad y Desviaciones Normativas

Cita Exacta / Ubicación	Vulnerabilidad y Desviación Técnica	Severidad	Estándar Violado
Página 2, Sección 2.3.1	**Almacenamiento S3 sin Cifrado en Reposo:** 3 buckets S3 que contienen datos sensibles de tarjetas (PAN) y PII de clientes carecen de cifrado activo mediante AWS KMS.	**CRÍTICA**	PCI-DSS v4.0 Req. 3.4 CNBV Art. 165
Página 3, Sección 2.3.2	**Llaves IAM con Privilegios Elevados sin MFA:** 14 llaves de acceso IAM con rol *AdministratorAccess* activas sin MFA y hardcoded en código fuente interno.	**CRÍTICA**	ISO 27001 A.9.4.2 CNBV Art. 168
Página 4, Sección 2.3.3	**Puertos de Gestión Expuestos en AKS:** Puertos SSH (22) y RDP (3389) abiertos a 0.0.0.0/0 en el clúster AKS de producción del Core Bancario.	**CRÍTICA**	ISO 27001 A.13.1.1 PCI-DSS Req. 1.3

Página 5 | Sección 3.2: Evaluación de Impacto Regulatorio y Sancionatorio

Las desviaciones críticas detectadas en las secciones 2.3.1 a 2.3.3 exponen a la institución a las siguientes consecuencias legales y operativas:

- **Riesgo de Multa Regulada (Página 5, Sección 3.2.1):** La CNBV contempla sanciones pecuniarias de hasta 100,000 UMA (~$10.8M MXN / ~$600k USD) por falta de controles de encripción en datos de usuarios.
- **Revocación de Certificación PCI-DSS (Página 5, Sección 3.2.2):** La exposición de datos unencrypted (Sección 2.3.1) puede provocar la suspensión inmediata de procesamiento de tarjetas de crédito por parte del adquirente.
- **Riesgo de Intrusión y Ransoware (Página 5, Sección 3.2.3):** La apertura de los puertos SSH/RDP en AKS (Sección 2.3.3) representa un vector de ataque directo para secuestro de datos en el Core Bancario.

Página 6 | Sección 4.1: Plan de Remedición de Seguridad en la Nube

Para garantizar una postura defensiva antes de la inspección regulatoria, se establece la siguiente matriz de remediación obligatoria:

Fase de Ejecución	Acción Técnica de Remedición	Hallazgo Atendido	SLA Máximo

Fase 1: Inmediata	1. Activar cifrado predeterminado en buckets S3 usando AWS KMS. 2. Revocar llaves IAM hardcoded e imponer autenticación MFA obligatoria. 3. Modificar Security Groups para cerrar puertos 22 y 3389 en AKS.	Sección 2.3.1 Sección 2.3.2 Sección 2.3.3	**24 a 72 Horas**
Fase 2: Corto Plazo	Implementar escaneo automatizado de código fuente (SAST/DAST) en el pipeline de CI/CD para evitar filtración de credenciales y desplegar AWS GuardDuty.	Sección 2.3.2	**15 Días**
Fase 3: Pre-Auditoría	Realizar prueba de penetración (*PenTest*) de caja negra sobre el clúster AKS y someter el informe a la auditoría de certificación PCI-DSS 4.0.	Sección 3.2.2	**30 Días**