Seguridad y privacidad en bases de datos en la era del Cloud Computing: una mirada al contexto salvadoreño

Dinora Elizabeth Sánchez de Morales (dinora.sanchez@univo.edu.sv)
Facultad de Ingeniería y Arquitectura, Universidad de Oriente

Resumen

La adopción del cómputo en la nube ha revolucionado la gestión de datos en las organizaciones al ofrecer escalabilidad, flexibilidad y eficiencia operativa. No obstante, esta transformación también presenta desafíos significativos en materia de seguridad y privacidad.

Este artículo analiza las amenazas más frecuentes durante la migración de bases de datos a entornos cloud en El Salvador, identificando brechas legales, técnicas y organizacionales. A través de revisión documental y entrevistas a especialistas, se proponen buenas prácticas para una migración segura y confiable, alineadas con estándares internacionales.

Palabras Clave: Cloud Computing, bases de datos, seguridad, privacidad, El Salvador, ISO 27001.

Introducción

El avance de la computación en la nube ha transformado radicalmente la manera en que las organizaciones almacenan y gestionan sus datos, especialmente por su capacidad de ofrecer servicios bajo demanda, escalabilidad y flexibilidad (Mell & Grance, 2011). En El Salvador, muchas instituciones están migrando sus bases de datos hacia plataformas cloud con el fin de optimizar recursos y reducir costos operativos. Sin embargo, esta transición tecnológica también plantea retos considerables en términos de seguridad y privacidad (Slingerland, 2023).

La información crítica, al transferirse por redes públicas o híbridas, queda expuesta a riesgos como accesos no autorizados, interceptaciones, pérdida de integridad y errores de configuración (DataSunrise, n.d.). Esto se ve agravado por la escasa capacitación técnica del personal salvadoreño y por la falta de marcos normativos sólidos en protección de datos personales (del Río, 2023).

2. Metodología

Se utilizó un enfoque cualitativo-descriptivo, desarrollando:

• Revisión bibliográfica y documental sobre cloud computing, seguridad de la información, legislación salvadoreña y estándares internacionales.

• Entrevistas semiestructuradas a especialistas y empresas en San Salvador con experiencia en migración de bases de datos a la nube.

• Análisis comparativo entre prácticas locales y buenas prácticas internacionales como ISO/IEC 27001, OWASP y NIST.

2.1 Cloud Computing y Bases de Datos

El cloud computing, definido por Mell y Grance (2011) como un modelo de acceso bajo demanda a recursos compartidos, ha evolucionado desde mainframes hasta soluciones modernas como AWS y Azure. Las bases de datos en la nube ofrecen ventajas como escalabilidad automática y alta disponibilidad, pero también introducen riesgos de seguridad (Slingerland, 2023).

2.2 Amenazas comunes

Las amenazas más comunes identificadas en las empresas salvadoreñas incluyen inyecciones SQL y NoSQL, abuso de privilegios, accesos no autorizados y malware (del Río, 2023; DataSunrise, n.d.). Además, muchas organizaciones carecen de auditorías efectivas y almacenan respaldos sin cifrado, lo cual facilita el robo de datos (DataSunrise, n.d.).
Según estadísticas recientes, el 82% de las brechas de datos globales en 2023 involucraron información almacenada en la nube (Smith, 2025), lo cual refuerza la urgencia de aplicar medidas de seguridad más estrictas.

2.3 Brechas institucionales y legales

En El Salvador, a pesar de la existencia de leyes como la Ley de Protección de Datos Personales (Decreto N.º 144) y la Ley de Ciberseguridad (Decreto N.º 143), aún no se ha desarrollado un marco legal específico para entornos cloud. Estas limitaciones generan incertidumbre jurídica y aumentan la vulnerabilidad de las organizaciones frente a ciberataques (Asamblea Legislativa de El Salvador, 2023).

3. Resultados

3.1 Principales Desafíos

• Configuraciones incorrectas: el 60% de los encuestados las señalaron como una causa principal de brechas.
• Falta de capacitación: 43% destacó la escasez de personal calificado.
• Ataques frecuentes: Inyección SQL(30%), phishing(25%) , y DDoS(20%).

3.2 Normativas y Buenas Prácticas

Un pequeño porcentaje de profesionales aplican estándares como la ISO/IEC 27001. OWASP y NIST son las guías más recomendadas para seguridad en APIs.

3.3 Beneficios del Cloud Computing

Un 70% de los encuestados consideran que la escalabilidad es uno de los mayores beneficios, y un 65% considera aque la reducción de costos destacó ahorros en infraestructura.

4. Discusión

Los resultados reflejan que la seguridad en la nube depende de tres pilares:

1. Tecnología: Cifrado, controles de acceso y auditorías.
2. Personas: Capacitación continua en seguridad.
3. Procesos: Adopción de normativas y gestión de riesgos.

Si bien los proveedores de servicios cloud, como Amazon Web Services, Google Cloud y Azure, ofrecen medidas avanzadas de seguridad, estas no sustituyen la responsabilidad que tienen las empresas sobre sus propios datos (Chaloupka, 2024). El modelo de responsabilidad compartida establece que tanto el proveedor como el cliente deben implementar medidas de protección. Las entrevistas realizadas revelaron que muchas PYMES salvadoreñas han adoptado servicios cloud sin una evaluación previa de riesgos ni un plan estructurado de migración, lo cual incrementa la posibilidad de brechas de seguridad. Además, la mayoría de los incidentes reportados tienen causas humanas: mal manejo de credenciales, errores de configuración o desconocimiento del funcionamiento de los servicios contratados (del Río, 2023; IBM X-Force, 2023).

5. Conclusiones

Las organizaciones salvadoreñas enfrentan riesgos críticos durante la migración a la nube, exacerbados por la ausencia de normativas locales claras y la escasez de personal especializado. Para mitigar estas vulnerabilidades, resulta imperativo adoptar buenas prácticas como el cifrado de datos, la autenticación multifactorial y auditorías continuas, así como impulsar políticas nacionales alineadas con estándares internacionales (ISO/IEC 27001, NIST) y programas de formación en ciberseguridad que fortalezcan las capacidades técnicas del país. Solo mediante un enfoque integral que combine tecnología, regulación y capacitación se podrá garantizar una transición segura hacia entornos cloud sin comprometer la confidencialidad, integridad o disponibilidad de los datos.

Referencias

Chaloupka, M. (2024). Cloud Security: Foundations and Frameworks. Safetica.
DataSunrise. (n.d.). Database Threats and Protection Measures.
del Río, J. (2023). Ciberseguridad en tiempos de transformación digital.
IBM X-Force. (2023). Threat Intelligence Index.
Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST.
Slingerland, E. (2023). Historia y evolución de la computación en la nube.