Lectura 10

Bases de Datos II

Luis Diego Delgado Muñoz

Prof. Nereo Campos

Fecha de Entrega: 31/05/2024

---

1. ¿Por qué se deben implementar controles que garanticen “compliance” en bases de datos?

La implementación de controles que garanticen "compliance" en bases de datos es esencial porque las bases de datos contienen grandes cantidades de datos altamente sensibles. Estas medidas aseguran que solo usuarios autorizados puedan acceder a la información, lo cual es crítico para proteger contra accesos no autorizados, fraudes y otros riesgos de seguridad. Además, muchas regulaciones de cumplimiento, como PCI DSS y HIPAA, tienen requisitos específicos sobre cómo deben gestionarse los accesos y las actividades dentro de las bases de datos.

2. ¿Qué papel juegan los sistemas de Observabilidad en garantizar el “compliance” con estándares como HIPAA y PCI DSS? Comente como los controles específicos pueden ser monitoreados con un sistema como Prometheus

Los sistemas de Observabilidad juegan un papel crucial en garantizar el compliance con estándares como HIPAA y PCI DSS al proporcionar visibilidad continua y en tiempo real de las actividades y eventos dentro de las bases de datos. Estos sistemas permiten detectar y responder rápidamente a actividades anómalas o no autorizadas, asegurando así que las medidas de seguridad y cumplimiento se mantengan efectivas.

Monitoreo con Prometheus: Prometheus puede ser utilizado para monitorear diversos controles específicos mediante la recolección y análisis de métricas y logs relevantes de las bases de datos. Algunas formas en que puede ayudar incluyen monitorear intentos de acceso y autenticaciones fallidas, supervisar y registrar todas las acciones y consultas realizadas por los usuarios, asegurando que se adhieran a las políticas definidas y verificar que las configuraciones de la base de datos no se hayan alterado y que se mantengan en línea con las políticas de seguridad.

3. ¿Por qué “Separation of Duties” es importante para el manejo de bases de datos? ¿Está bien que una persona tenga control completo sobre todos los sistemas?

La "Separation of Duties" (SoD) es crucial para el manejo de bases de datos porque reduce el riesgo de errores y fraudes. Al dividir responsabilidades y accesos entre diferentes individuos, se asegura que ninguna persona tenga control total sobre todos los aspectos de los sistemas, lo cual puede llevar a abusos de poder o a errores no detectados. Esto también facilita la detección y prevención de actividades fraudulentas, ya que las acciones de un individuo pueden ser revisadas y auditadas por otros.

4. Tomando en cuenta lo estudiado en clases acerca de seguridad de bases de datos (desde seguridad física hasta aplicación) y este artículo, ¿Qué controles consideran que fallaron dando como resultado el faltante de aproximadamente 3200 millones de

colones en el Banco Nacional? ¿Con lo estudiado en este curso qué controles y sistemas implementarían para evitar este tipo de problemas?

Controles que fallaron:

1. **Seguridad Física**: Probablemente hubo deficiencias en la seguridad física de la bóveda, permitiendo acceso no autorizado.
2. **Autenticación y Control de Accesos**: Falta de medidas estrictas de autenticación y control de accesos a las áreas y sistemas críticos.
3. **Monitoreo y Auditoría**: Posiblemente, hubo insuficiente monitoreo y auditoría de las actividades dentro de la bóveda y en las bases de datos.
4. **Separation of Duties**: La falta de separación de responsabilidades pudo haber permitido que una o pocas personas manejaran transacciones críticas sin supervisión adecuada.

Controles y sistemas para implementar:

1. **Refuerzo de Seguridad Física**: Instalar cámaras de seguridad, sistemas de alarmas y controles de acceso biométricos en áreas sensibles.
2. **Autenticación Multi-Factor (MFA)**: Implementar MFA para acceder a sistemas críticos y áreas restringidas.
3. **Monitoreo Continuo**: Utilizar sistemas de monitoreo en tiempo real como Prometheus para vigilar todas las actividades en la base de datos y generar alertas ante comportamientos anómalos.
4. **Auditorías Regulares**: Realizar auditorías periódicas y aleatorias de las transacciones y accesos a las bases de datos.

Estos y muchos otros controles y sistemas ayudarían a reducir significativamente los riesgos de fraude y errores, mejorando la seguridad y el cumplimiento en las operaciones del Banco Nacional.