10 de diciembre del 2024

AI-0231-2024

Señora

Hazel Valverde R., Gerente

**BANCO CENTRAL DE COSTA RICA**

**Ref. Comunicación del informe de la auditoría especial sobre la gestión de bases de datos**

Estimada señora:

Este informe contiene los resultados y anexos correspondientes al estudio de carácter especial[[1]](#footnote-1), mediante el cual esta Auditoría evaluó la gestión de bases de datos y cuyo objetivo fue verificar el cumplimiento de las disposiciones aplicables al proceso, el cual está bajo la responsabilidad del Departamento de Ciencia e Ingeniería de Datos de la División de Servicios Tecnológicos.

El alcance del estudio comprendió la administración de accesos, las modificaciones directas a los datos y la gestión de respaldos de enero a septiembre del 2024; se excluyó la gestión del lago de datos pues ya había sido auditado recientemente[[2]](#footnote-2). Para la ejecución de este estudio se aplicaron los criterios de auditoría que se consideraron pertinentes, según el objetivo planteado, los cuales fueron comunicados mediante oficio AI-0220-2024 del 25 de noviembre del 2024.

La actividad de auditoría interna en el Banco Central de Costa Rica se realiza de acuerdo con las Normas para el Ejercicio de la Auditoría Interna en el Sector Público y las Normas Generales de Auditoría para el Sector Público, ambas emitidas por la Contraloría General de la República.

Los resultados obtenidos permitieron concluir que el proceso evaluado **cumple** con los criterios de evaluación establecidos.

# GENERALIDADES

Las bases de datos desempeñan un papel crucial en el Banco Central de Costa Rica (BCCR), ya que almacenan y protegen información crítica relacionada con sus operaciones. Esto incluye transacciones financieras, datos económicos, registros internos y datos sensibles de los usuarios. Una gestión adecuada de estas bases de datos garantiza su disponibilidad, integridad y confidencialidad, factores esenciales para el cumplimiento de los objetivos del banco y para mantener la confianza de los ciudadanos y entidades financieras adscritas a los servicios de la institución como SINPE, Central Directo, Firma Digital. Por el contrario, una falla en su gestión podría ocasionar interrupciones significativas en los servicios, pérdida de información, o riesgos operativos y de seguridad.

Actualmente, el BCCR dispone de una estructura de gestión de bases de datos, tanto en instalaciones locales como en la nube, centralizada bajo la responsabilidad de su Departamento de Ciencia e Ingeniería de Datos. Este departamento se encarga de las actividades de administración, optimización y protección de los datos utilizando tecnologías como SQL Server y Always On Availability Groups[[3]](#footnote-3) para alta disponibilidad.

# RESUMEN DE RESULTADOS

Los resultados de esta evaluación permitieron identificar los siguientes aspectos:

**Administración de accesos a los datos**

1. Se constató que el Banco cuenta con políticas y procedimientos establecidos para regular el acceso a las bases de datos. Dichos accesos son otorgados conforme el principio de mínimo privilegio, asegurando que los roles y permisos asignados correspondan únicamente a las necesidades específicas de cada usuario.
2. Se constató que el Departamento de Ciencia e Ingeniería de Datos dispone de un procedimiento formal para gestionar los accesos a las bases de datos en ambientes de no producción, asegurando un control adecuado y alineado con las mejores prácticas.
3. Se observó que el Banco implementó un monitoreo activo para identificar y prevenir accesos no autorizados a los datos críticos, fortaleciendo así la seguridad de la información.
4. Se confirmó que el Banco cuenta con procedimientos establecidos para desactivar o eliminar cuentas de usuario inactivas, garantizando un control efectivo sobre el acceso a los sistemas y la protección de la información.

**Modificaciones directas de datos**

1. Se constató que el Departamento de Ciencia e Ingeniería de Datos cuenta con procedimientos y guías formales para la gestión de modificaciones a la estructura de las bases de datos. Estos incluyen mecanismos para solicitar, aprobar y documentar las modificaciones realizadas a las estructuras, así como para revertir cambios en caso de ser necesario, asegurando un control adecuado y trazabilidad en estas operaciones.
2. Se verificó que el Departamento de Ciencia e Ingeniería de Datos dispone de procedimientos establecidos para realizar cambios directos a los datos. Estos procedimientos incluyen actividades para solicitar, aprobar, y documentar los cambios solicitados a los datos, garantizando la trazabilidad mediante el registro de detalles como el propósito de la modificación, la fecha en que se realizó, y la identificación del responsable.

**Administración de respaldos**

1. Se constató que el Banco cuenta con una política de Ciberseguridad que abarca la gestión de respaldos de las bases de datos, incluyendo los períodos de retención y los métodos de protección de los datos respaldados. Además, se verificó que cada propietario de los datos es responsable de definir la frecuencia de los respaldos de las bases de datos asociadas a sus sistemas.
2. Se verificó que el Banco cuenta con una infraestructura adecuada para gestionar los respaldos y están protegidos contra accesos no autorizados.
3. Se constató que en el Banco realiza pruebas periódicas de restauración de respaldos, asegurando la funcionalidad y confiabilidad de los mecanismos de recuperación de datos.
4. Se comprobó que el plan de recuperación ante desastres para las bases de datos está alineado con los objetivos de continuidad operativa del Banco y permite, de manera razonable, una recuperación efectiva dentro de los límites de tiempo aceptables.

La Auditoría Interna realizó la conferencia final de este informe con la División de Servicios Tecnológicos y con la Gerencia, como parte de la comunicación preliminar de los resultados.

Atentamente,



Maribel Lizano Barahona

**Subauditora Interna**

Cc. División Servicios Tecnológicos

1. La auditoría de carácter especial, conocida también como auditoría de cumplimiento, se enfoca en determinar si las actividades se ejecutan de conformidad con las leyes, reglamentos u otras normativas que las regulan, tales como resoluciones, políticas, lineamientos, directrices, códigos, contratos, convenios, u otros criterios considerados apropiados por el auditor. Estas auditorías de cumplimiento pueden abarcar una extensa gama de materias controladas, tales como aspectos de orden contable-financiero, presupuestario, administrativo, económico, estadístico, jurídico, control interno y otras temáticas relacionadas con la fiscalización pública. [↑](#footnote-ref-1)
2. Oficios AI-0052-2024 y AI-0133-2024, del 12/03/2024 y 29/07/2024, respectivamente. [↑](#footnote-ref-2)
3. Funcionalidad avanzada de alta disponibilidad y recuperación ante desastres ofrecida por Microsoft SQL Server a partir de la versión 2012. [↑](#footnote-ref-3)