18 de setiembre del 2024

AI-0166-2024

Señora

Hazel Valverde R., Gerente

**BANCO CENTRAL DE COSTA RICA**

Estimada señora:

Este informe presenta los resultados y anexos correspondientes al estudio operativo[[1]](#footnote-1) realizado por esta Auditoría, cuyo objetivo fue evaluar la eficacia del proceso de gestión de telecomunicaciones en relación con los riesgos relevantes y el sistema de control interno. Dicho proceso está bajo la responsabilidad del Departamento de Infraestructura Tecnológica, perteneciente a la División de Servicios Tecnológicos.

El alcance del estudio comprendió las operaciones realizadas durante el año 2023.

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 la gestión de telecomunicaciones **es eficaz** pues se observó que la aplicación del marco regulatorio, la gestión de infraestructura y tecnología de las redes, la gestión de la seguridad, así como la gobernanza y estrategia implementadas cuentan con controles eficaces y adecuados para mitigar de manera razonable los riesgos relevantes.

# GENERALIDADES

En el Banco Central de Costa Rica, la gestión de las telecomunicaciones es una responsabilidad del Departamento de Infraestructura Tecnológica (DIT) que pertenece a la División se Servicios Tecnológicos. Su objetivo es garantizar un entorno que sea seguro, ágil, confiable, robusto y escalable, en apoyo a las operaciones y al crecimiento organizacional. Esta administración se lleva a cabo de manera centralizada, siguiendo las mejores prácticas para la gestión de la plataforma, la administración de la configuración y el entorno, e incluye la gestión de los equipos de comunicación, telefonía y enlaces.

El departamento también es responsable de establecer los requerimientos necesarios para el funcionamiento óptimo de los centros de datos y cuartos de cableado, autorizando y supervisando los trabajos de mejora y mantenimiento que son esenciales para minimizar posibles incidentes. Asimismo, el DIT cuenta con herramientas especializadas para monitorear el rendimiento de los equipos que soportan la red del Banco, incluyendo enlaces, enrutadores, switches, red inalámbrica e Internet, entre otros.

# RESUMEN DE RESULTADOS

Los resultados de esta evaluación fueron:

1. La estrategia de telecomunicaciones del plan táctico de la División de Servicios Tecnológicos (DST) está razonablemente alineada con los objetivos generales del Banco.
2. El DIT, en conjunto con el Departamento de Gestión de Riesgos y Cumplimiento, tiene actualizado el ejercicio de riesgo a febrero de este año; tal ejercicio muestra que los niveles de riesgos residual son aceptables, por lo que no hay pendientes de ejecutar planes de mitigación.
3. El DIT aplica las políticas institucionales establecidas para la gobernanza de TI, la seguridad de la información y la ciberseguridad. Además, ese departamento ha definido y aplica satisfactoriamente procedimientos operativos y guías de trabajo para la gestión de incidentes y solicitudes, así como para la gestión de cambios, asegurando que estos sean revisados y aprobados antes de su implementación en los entornos de producción.
4. Se realizan copias de seguridad de la configuración de los equipos de telecomunicaciones antes de efectuar cualquier cambio, y se cuenta con un plan de recuperación para abordar posibles problemas que pudieran surgir durante el proceso.
5. Se coordinan ventanas de tiempo con la administración para llevar a cabo tareas de mantenimiento, instalación o gestión de cambios en la infraestructura de telecomunicaciones. Estas labores incluyen un análisis del impacto de cada tarea individual, determinando cuáles pueden realizarse durante el horario hábil y cuáles requieren la utilización de la ventana de mantenimiento.
6. Tras la implementación de cambios, se realizan verificaciones del acceso a sistemas y servicios para asegurar su correcto funcionamiento.
7. Se implementan planes de pruebas de negocio, acompañado de la correspondiente aprobación antes de su ejecución.
8. Se realizan procedimientos adecuados para la habilitación o deshabilitación de puertos para los equipos de telecomunicaciones.
9. Los cambios realizados en la infraestructura Azure son verificados para asegurar su correcta implementación y funcionamiento.
10. Se emplean herramientas de monitoreo en tiempo real y se han implementado procedimientos eficaces para detectar, responder y documentar incidentes operativos y de ciberseguridad de manera ágil y oportuna.
11. En cuanto a las medidas de seguridad física, se dispone de controles de acceso físico, herramientas de monitoreo de ingresos y sistemas de detección de intrusiones.
12. La documentación detallada de la topología de las redes del Banco se encuentra actualizada.

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 de Servicios Tecnológicos

1. Auditoría operativa: Evalúa la eficacia, eficiencia o economía con que la entidad, programa, proyecto, unidad, proceso o actividad utiliza los recursos públicos para el desempeño de sus cometidos. [↑](#footnote-ref-1)