



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincecss@ccss.sa.cr

Al contestar refiérase a: **ID-137625**

AS-ATIC-0056-2025

21 de mayo de 2025

Licenciado

Ronald Lacayo Monge, director

Ingeniero

Ciro Gómez Rodríguez, jefe CGI

DIRECCIÓN REGIONAL DE SUCURSALES CHOROTEGA - 1401

Licenciado

Roberth Chavarría Ruiz, administrador

SUCURSAL LIBERIA - 1408

Estimados señores:

ASUNTO: Oficio de Asesoría sobre la continuidad del negocio ante fallas en la comunicación y lentitud de sistemas en la sucursal de Liberia.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2025 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, específicamente en su rol de asesor, esta Auditoría tuvo conocimiento del "COMUNICADO DE PRENSA", suscrito por el Lic. Jonathan Reina Canales, Administrador a.i., de la sucursal de Liberia, en el cual se informó sobre "Fallas en la comunicación telefónica y posible lentitud en sistemas por avería en el switch de la Sucursal de Liberia".

1. Antecedentes

El 24 de marzo de 2025, mediante WebMaster, se emite comunicado de prensa de la Sucursal de Liberia, en el cual se describe lo siguiente:

"La Sucursal de Liberia de la Caja Costarricense de Seguro Social (CCSS) informa a sus usuarios que se han detectado fallas en el switch de telecomunicaciones, un componente clave que gestiona el enrutamiento de llamadas y la conectividad de los sistemas internos.

Debido a esta avería, se están presentando interrupciones intermitentes en la comunicación telefónica, lo que podría ocasionar que algunas llamadas ingresen con normalidad mientras que otras no se completen correctamente. Además, esta situación puede generar lentitud en los sistemas informáticos de la sucursal.

Actualmente, estamos trabajando en el proceso de reemplazo del switch para restablecer la estabilidad en los servicios de telecomunicaciones y sistemas. Pedimos disculpas por los inconvenientes que esto pueda causar y agradecemos la comprensión de nuestros asegurados.

Estamos haciendo todo lo posible para minimizar las afectaciones y garantizar que la normalidad se restablezca a la mayor brevedad. Para consultas o trámites urgentes, los usuarios pueden dirigirse personalmente a nuestra sucursal en el horario habitual de atención o a los siguientes correos..."

En virtud de lo anterior y con propósito de garantizar la continuidad de los servicios, el 25 de marzo de 2025, esta Auditoría consultó al Lic. Reina Canales, Administrador a.i., de la sucursal de Liberia, sobre el origen y el procedimiento de atención de la incidencia, señalando al respecto:

“El incidente ocurrió el 19 de marzo de 2025, cuando la Sucursal de Liberia experimentó un fallo en un switch, lo que limitó ciertos accesos. Sin embargo, el departamento de CGI intervino de inmediato para solucionar el problema, trabajando incluso el 20 de marzo para restablecer el servicio. Durante este período, el equipo de informática implementó ajustes en los sistemas de comunicación para minimizar el impacto en la atención a los usuarios...”

...el 24 de marzo de 2025, se registraron problemas de comunicación telefónica intermitente, donde algunas llamadas entraban y otras no. El equipo de informática indicó que el cambio del switch estaba en trámite para resolver la situación.

Ese mismo día, el jefe de informática de la Dirección Regional Sucursales Chorotega (DRSCH)... comunicó que, debido a la urgencia, el cambio del switch se realizaría el 25 de marzo de 2025”.

El 27 de marzo de 2025, el Lic. Reina, por medio de la Plataforma Microsoft Teams, informó sobre la resolución definitiva de la incidencia, mencionando: **“ayer (26/03/2025) se solucionó el problema de comunicación de la Sucursal de Liberia, todo bien 100 %”.** (Lo negrita no es del original).

2. Consideraciones Normativas

El artículo 8 de la Ley General de Control Interno, respecto al sistema de control interno, establece:

“(...) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

- a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*
- b) Exigir confiabilidad y oportunidad de la información.*
- c) Garantizar eficiencia y eficacia de las operaciones.*
- d) Cumplir con el ordenamiento jurídico y técnico (...)”*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el apartado XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, lo siguiente:

“La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.

La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.

La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción”.

Las Políticas de Seguridad Informática institucionales (octubre 2007) establecen en su apartado 10.14 Política para la elaboración de Planes de Continuidad de la Gestión, lo siguiente:

“Los Planes de Continuidad de la Gestión, deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Adicionalmente como los planes de continuidad de la gestión pueden fallar debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, debe considerarse dentro de su administración la realización de pruebas periódicas para garantizar que los mismos estén actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes”.

Según el marco referencial COBIT 2019 (Objetivos de gobierno y gestión), en la descripción del proceso DSS04, DSS04.02 y DSS04.04 se indica lo siguiente:

“Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa.

Evaluar las opciones de resiliencia del negocio y elegir una estrategia viable y rentable para asegurar la continuidad, la recuperación ante un desastre y la respuesta ante incidentes de la empresa ante un desastre u otro incidente o interrupción mayor.

Probar la continuidad de forma periódica para ver el comportamiento de los planes contra resultados predeterminados, mantener la resiliencia del negocio y permitir que se desarrollen soluciones innovadoras”.

3. Productos de Auditoría emitidos sobre la continuidad del negocio

La Auditoría Interna ha señalado a la Administración la relevancia de examinar lo correspondiente a la continuidad del negocio y la contingencia de los servicios tecnológicos, efectuando observaciones que permitan atender oportunidades de mejora aplicables al proceso y así disponer de medidas acorde a las necesidades de la Institución.

El Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico, AS-AATIC-088-2022, del 16 de junio de 2022, en el punto 3, Consideraciones Finales, cita:

“La Caja Costarricense del Seguro Social (CCSS), dentro de su gestión y servicios que presta a la ciudadanía depende de la información, sistemas y soluciones tecnológicas, entre otros procesos; de ahí la necesidad de disponer de un sistema de gestión para la continuidad del negocio.

Lo anterior, en aras de que la Institución en cada uno de los procesos de salud, pensiones y recaudación patronal disponga de herramientas o soluciones capaces de aportar valor cuando las actividades sustantivas permanezcan ininterrumpidas, por fallas de origen eléctrico, financiero, tecnológico, eventos de seguridad, desastres naturales, entre otros”.

Asimismo, el Oficio de Asesoría referente a los Planes de Continuidad de TIC, AS-AATIC-116-2022, del 7 de julio de 2022, en el apartado IV. Consideraciones, describe:

“Los Planes de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, deben tener como objetivo garantizar la recuperación de los equipos y sistemas críticos posterior a la materialización de un riesgo, además de establecer políticas y procedimientos que reduzcan en la medida de lo posible la afectación o suspensión de los servicios que se brindan a los usuarios.

Dentro de ese orden de ideas, se debe destacar que los beneficios de contar con un plan de continuidad en TIC se resumen en la gestión adecuada de los riesgos, reducción de los períodos de interrupción y mejora en la calidad de los servicios”.

4. Observaciones

En este contexto, la Auditoría Interna se refiere al argumento señalado en el epígrafe, con el propósito de que esa Administración defina estrategias frente a los eventos recientes y aquellos que pudieran presentarse en el futuro. Lo anterior, considerando la importancia de asegurar la continuidad operativa del negocio y el impacto derivado de fallas en los dispositivos tecnológicos, entre otros, cuya reiteración no pueden descartarse.

4.1 Sobre el plan de continuidad de la gestión en TIC y sus mecanismos de contingencia

Con respecto al plan de contingencia implementado y si funcionó en el manejo de la falla presentada en la sucursal de Liberia, el Lic. Jonathan Reina Canales, Administrador a.i., de la sucursal de Liberia, informó que la atención fue inmediata por parte del departamento de informática, quienes implementaron ajustes en los sistemas de comunicación para mitigar el impacto en la atención a los usuarios. Asimismo, sobre si se documentó el hecho para minimizar el riesgo de recurrencia y procurar el aprendizaje ante eventos similares, el Lic. Reina Canales, señaló que la falla fue comunicada de inmediato a la administración y, solicitará al departamento de informática un informe detallado del incidente para su documentación.

El Ing. Ciro Gómez Rodríguez, jefe del Centro de Gestión Informática de la Dirección Regional de Sucursales Chorotega, sobre el particular, informó:

“La falla está plenamente identificada, se sustituye temporalmente el equipo (Switch), gracias a la colaboración por parte de personeros del CGI del Hospital Monseñor Sanabria, todo el evento será documentado y remitido mediante informe, toda vez que se brinde la solución, ya que en estos momentos aun nos encontramos en la atención de la incidencia”.

El 10 de abril de 2025, mediante oficio DRSCH-AGI-0027-2025 del 10 de abril de 2025, el Ing. Steven Roberto Vargas Barrantes, del Centro de Gestión informática de la Dirección Regional Sucursales Chorotega, emitió al Lic. Roberth Antonio Chavarría Ruíz, Administrador de la Sucursal de Liberia, el “Informe de visita a la sucursal de Liberia – cambio UPS OnLine”, señalando en el apartado de conclusiones, lo siguiente:

“El cambio de UPS y la reconfiguración del switch de inspección como switch principal realizado el 20 de marzo del presente año fueron soluciones temporales que permitieron recuperar la conectividad en la sucursal.

La instalación del switch (placa 1379480) instalado el 25 de marzo del presente año, prestado por parte del hospital Monseñor Sanabria permitió restablecer la red en su totalidad con red alámbrica”.

En línea con lo anterior, esta Auditoría evidenció que el Plan de Continuidad de la Gestión de los Servicios TIC de la Sucursal de Liberia, requiere mejorarse, así señalado en el oficio GG-DTIC-0877-2025 del 18 de febrero de 2025, “Informe hallazgos y recomendaciones: “Plan de Continuidad de los Servicios TIC”, elaborado por la Ing. Aldania Arias Vargas, del Área de Seguridad y Calidad Informática, y dirigido al Lic. Robert Chavarria Ruiz, Administrador de la Sucursal de Liberia y al Lic. Angel Esteban Morales Noguera, jefe Centro de Gestión Informática de la Dirección Regional de Sucursales Chorotega, señalando en el apartado de conclusiones, lo siguiente:

“Es criterio de esta Área que el nivel de preparación del Plan de Continuidad de la Gestión de los Servicios TIC de la Sucursal de Liberia “necesita mejorarse”, como resultado de la aplicación de la evaluación respectiva.

Se considera que el documento presentado cumple con el modelo establecido en el manual para elaboración de los Planes de Continuidad, sin embargo, se debe seguir trabajando en el desarrollo enfocado en realizar mejoras según los hallazgos identificados, documentar la gestión de riesgos, la ejecución y documentación de ensayos, y en las actualizaciones o mantenimiento anual al plan.

Todos los puntos señalados en la sección de hallazgos incluyen una acción pendiente a desarrollar por parte de la unidad, para lo cual deben realizar una subsanación al documento.

*Se establece como fecha límite de entrega con las correcciones solicitadas a más tardar **el 28 de marzo 2025**”.*

El 4 de abril de 2025, mediante oficio GG-DTIC-2110-2025, la Ing. Aldania Arias Vargas, del Área de Seguridad y Calidad Informática, informo al Ing. Ciro Gómez Rodríguez, jefe Centro de Gestión Informática de la Dirección Regional de Sucursales Chorotega, en respuesta al oficio DRSCH-AGI-0023-2025, Solicitud prórroga de plazo para entrega de modificaciones PCSTIC, lo siguiente:

*Se recibe oficio DRSCH-AGI-0023-2025 con fecha 02 de abril 2025, mediante el cual realiza solicitud de ampliación en plazo de la entrega de las modificaciones al Plan de Continuidad de los Servicios TIC. Al respecto, **se amplía el plazo de entrega para el 09 de mayo 2025 a más tardar...**”.*

Ante la falla técnica presentada en la sucursal de Liberia, se evidenció una respuesta inmediata y efectiva por parte del área de Informática de la Dirección Regional de Sucursales Chorotega, quienes implementaron acciones correctivas para mitigar el impacto operativo. Las medidas adoptadas, entre ellas la reconfiguración del sistema de comunicación y el reemplazo temporal de equipo crítico, permitieron mantener la continuidad mínima de los servicios, lo cual refleja un nivel adecuado de coordinación técnica y compromiso con la continuidad del negocio. Sin embargo, cabe señalar que las soluciones implementadas fueron de carácter provisional, lo cual pone de manifiesto la necesidad de contar -en términos de eficiencia, eficacia y economía- con recursos tecnológicos críticos disponibles de forma anticipada, a fin de reducir la dependencia de apoyos externos y fortalecer la resiliencia institucional.

En cuanto al proceso de documentación del incidente, se destaca que el mismo fue comunicado de manera oportuna a las autoridades administrativas correspondientes, solicitando la elaboración de un informe técnico detallado para registrar formalmente lo acontecido, el cual se comunicó el 10 de abril de 2025, formando una buena práctica para la consolidación de evidencias y la retroalimentación del proceso de mejora. No obstante, se identifica como área de mejora el hecho de que dicha documentación haya sido gestionada de manera reactiva, y no como parte de un procedimiento estructurado previamente contemplado en el Plan de Continuidad. Asimismo, no se reporta la existencia de ejercicios previos de simulación o validación del plan, lo cual limita la capacidad institucional de anticipación, aprendizaje organizacional y de cuantificar tiempos de respuesta.

El análisis efectuado por el Área de Seguridad y Calidad Informática mediante el informe GG-DTIC-0877-2025 concluye que el Plan de Continuidad de los Servicios TIC de la Sucursal de Liberia requiere oportunidades de mejora. Si bien el documento cumple con el formato y modelo establecido en el manual institucional, se identifican deficiencias relevantes en cuanto a su contenido y aplicación práctica. Entre los aspectos críticos detectados se encuentran la falta de una adecuada gestión documental de riesgos, definición de los tiempos de recuperación, la ausencia de ejecución y registro de pruebas o simulacros, así como la inexistencia de un proceso sistemático de actualización y mantenimiento anual. Esta situación representa una vulnerabilidad significativa en términos de preparación y capacidad de respuesta ante eventos de contingencia.

En atención a las mejoras sustanciales señaladas, la Sucursal de Liberia en conjunto con el Centro de Gestión Informática de la Dirección Regional de Sucursales Chorotega, han iniciado un proceso de mejora, con el objetivo de subsanar las deficiencias detectadas. No obstante, dicho proceso ha requerido la solicitud de una prórroga para cumplir con las correcciones indicadas, situación formalizada mediante el oficio DRSCH-AGI-0023-2025. La



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

ampliación del plazo otorgada hasta el 9 de mayo de 2025 evidencia la voluntad institucional de atender las observaciones, aunque también refleja retrasos en la implementación de las acciones correctivas dentro del marco temporal inicialmente establecido. Este hecho destaca la importancia de fortalecer los mecanismos de planificación, seguimiento y control del cumplimiento de los planes de continuidad, garantizando así su vigencia, eficacia y alineamiento con los estándares de calidad y seguridad de los servicios TIC.

5. Consideración final

Así las cosas, es necesario la necesidad de disponer de un Plan de Continuidad de la Gestión en Servicios de Tecnologías de la Información y Comunicaciones (TIC) debidamente documentado, actualizado y alineado con las necesidades operativas de la institución, el cual se constituya en un componente esencial para la gestión de riesgos y la resiliencia de la unidad y de la organización. Asimismo, contar con mecanismos de contingencia eficaces permite mantener la operación de las actividades sustantivas ante interrupciones provocadas por fallas de origen eléctrico, financiero, tecnológico, incidentes de seguridad, desastres naturales u otros eventos imprevistos. En consecuencia, la preparación y capacidad de respuesta ante estos escenarios no solo mitigan impactos negativos, sino que también aportan valor estratégico al garantizar la continuidad de los servicios institucionales.

En esa misma línea, y en apego al artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones que se ejecuten, resulta fundamental que la administración activa se mantenga vigilante de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias, a fin de garantizar razonablemente la recuperación y continuidad de los servicios ante este tipo de imprevistos, de modo que su interrupción no afecte significativamente a sus usuarios.

Atentamente,

AUDITORÍA INTERNA



Lic. Randall Jiménez Saborio. MATI
Sub Auditor

OSC/RJS/RAHM/OCA/ayms

C. Auditoría

Referencia: ID-137625