CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: coinccss@ccss.sa.cr

ATIC-0113-2023
14 de diciembre de 2023

RESUMEN EJECUTIVO

El presente estudio fue realizado de acuerdo con el Plan Anual Operativo 2023 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar el restablecimiento de sistemas y servicios tecnológicos posterior al ciberataque del 2022.

Cualquier organización está expuesta a diversos factores que podrían afectar la continuidad del negocio, tales como: desastres naturales, incidentes ambientales, pandemias, conflictos laborales, dificultades financieras, atrasos o demoras en la cadena de suministro, problemas de seguridad física, complicaciones tecnológicas, eventos sociopolíticos, desastres humanos, entre otros no menos importantes. En este contexto, es de vital importancia tomar las medidas pertinentes para prevenir su materialización y, en caso de ocurrir, reducir significativamente su impacto, permitiendo así la gestión eficiente del restablecimiento de servicios vinculados a los procesos operativos.

Bajo esa perspectiva, se identificaron oportunidades de mejora aplicables, tanto a nivel estratégico y táctico de la institución, involucrando a los responsables en el ámbito de negocio, como en el tecnológico. A este respecto, se evidenció que el Programa de Gobernanza y Gestión de las TIC, propuso el desarrollo de la iniciativa “Habilitar la gestión de la continuidad del negocio”; sin embargo, desde 2018 hasta la fecha no ha iniciado su desarrollo.

Esta situación presenta desafíos significativos para la CCSS, debido a la limitación que se está dando para obtener a la brevedad los beneficios relacionados con la garantía razonable de establecer actividades para impulsar la continuidad del negocio. Asimismo, pone en riesgo la capacidad de la institución para atender recomendaciones y propuestas basadas en las mejores prácticas; lo anterior, considerando que, a lo largo del tiempo, la Caja no ha logrado adoptarlas en lo correspondiente a la seguridad de la información y la continuidad del negocio.

Por otra parte, durante y/o posterior al ciberataque perpetrado en mayo de 2022, no se llevó a cabo evaluaciones integrales y estandarizadas que detallaran las áreas afectadas a nivel institucional en términos de productividad, reputación, aspectos normativos, entre otros. A pesar de los esfuerzos realizados para generar informes desde los ámbitos tecnológico y financiero en la CCSS, se evidencia la carencia de una metodología que respalde el despliegue oportuno de información estandarizada referente a la emergencia, dificultando la realización de un análisis multidisciplinario detallado, necesario para respaldar la toma de decisiones en el ámbito estratégico y táctico.

En consonancia con lo anterior, los hallazgos de la evaluación revelan la inexistencia de un plan de fortalecimiento en lo que refiere a la postura institucional (a nivel de negocio) orientado a mejorar y consolidar la reputación y credibilidad; capacidad de resiliencia en escenarios adversos; manejo de crisis; alineación estratégica; entre otros aspectos que construyen una imagen sólida, auténtica y positiva sobre la gestión institucional y no solamente en materia de Ciberseguridad.

En relación con la Subárea de la Continuidad de la Gestión, se evidencian limitaciones sustanciales derivadas de la disponibilidad de personal y su debilitamiento debido al traslado del único recurso disponible para atender el ciberataque. Este escenario ha llevado a la paralización de funciones fundamentales durante más de 17 meses, incluyendo las evaluaciones a los planes de continuidad en el ámbito de las Tecnologías de la Información a nivel institucional.

En cuanto al marco normativo aplicable a la temática analizada en el presente informe, se observa su desactualización por amplios periodos de tiempo, lo cual representa un riesgo a la premisa de asegurar que la regulación respalde el proceso y se ajuste a las necesidades actuales.

En virtud de lo expuesto, este Órgano de Fiscalización ha solicitado al Consejo Tecnológico de la CCSS; Centro de Atención de Emergencias y Desastres; y a la Dirección de Tecnologías de Información y Comunicaciones se adopten acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable y así coadyuvar en el fortalecimiento de las estrategias, alineamiento de las TI y el uso adecuado de los recursos institucionales; bajo principios de eficiencia, eficacia y cumplimiento del ordenamiento jurídico-técnico.

AATIC-0113-2023
14 de diciembre de 2023

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE EL RESTABLECIMIENTO DE SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS POSTERIOR AL CIBERATAQUE DEL 2022 - PRESIDENCIA EJECUTIVA - 1102, CENTRO DE ATENCIÓN DE EMERGENCIAS Y DESASTRES - 1170, DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo 2023 para el Área de Auditoría de Tecnologías de Información y Comunicaciones en el apartado de estudios especiales.

OBJETIVO GENERAL

Evaluar el restablecimiento de sistemas de información y servicios tecnológicos posterior al ciberataque del 2022.

OBJETIVOS ESPECÍFICOS

- Identificar los mecanismos de control para diagnosticar la afectación a nivel tecnológico y de negocio en la CCSS, a partir del ciberataque ocurrido en mayo de 2022.

- Verificar el proceso de análisis y gestión de la información realizado hasta lograr la restauración de los servicios de Tecnologías de la Información y Comunicación (TIC) y sistemas de información institucionales.

- Comprobar las medidas adoptadas para prevenir la interrupción de servicios y sistemas institucionales en posibles situaciones similares en el futuro.

NATURALEZA Y ALCANCE

El estudio comprende la verificación de las acciones efectuadas por la Administración Activa en relación con el cumplimiento del marco normativo en la restauración de sistemas y servicios tecnológicos después del ciberataque ocurrido en 2022.

El periodo de evaluación incluye desde el 31 de mayo del 2022 al 20 de noviembre del 2023, ampliándose en los casos donde se consideró necesario.

Lo anterior, de acuerdo con lo dispuesto en las Normas Generales de Auditoría para el Sector Público y Normas para el Ejercicio de la Auditoría Sector Público, divulgadas a través de la Resolución R-DC-064-2014 de la Contraloría General de la República, publicadas en La Gaceta 184 del 25 de setiembre 2014, vigentes a partir del 1º de enero 2015 y demás normativa aplicable.

METODOLOGÍA

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Solicitudes y análisis de información formuladas por la Auditoría Interna, con las correspondientes respuestas proporcionadas por la Administración Activa a través de correo electrónico y en formato digital, en relación con las medidas adoptadas para la recuperación de sistemas de información y servicios tecnológicos tras el ciberataque de 2022, incluyendo:

  - ✓ Oficio AI-2181-2023 del 2 de noviembre del 2023, enviado a la Presidencia Ejecutiva; respondido en oficio GG-DTIC-7549-2023 del 10 de noviembre del 2023, suscrito por el Máster Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones y GG-1365-2023 del 27 de noviembre de 2023, suscrito por el Máster Juan Ignacio Monge Vargas, Jefe de Despacho de la Gerencia General.
  - ✓ Oficio AI-2182-2023 con fecha del 2 de noviembre de 2023, remitido al Cuerpo Gerencial de la Institución. Se recibieron respuestas en los oficios GA-2141-2023 (6 de noviembre de 2023), GF-4333-2023 (10 de noviembre de 2023), GIT-1885-2023 (10 de noviembre de 2023), GM-16655-2023 (10 de noviembre de 2023), GL-1969-2023 (11 de noviembre de 2023) y GP-1768-2023 (15 de noviembre de 2023).
  - ✓ Oficio AI-2301-2023 del 14 de noviembre del 2023, enviado al Área de Seguridad y Calidad Informática de la DTIC; respondido
  - ✓ Solicitud de información mediante correo electrónico del 6 de noviembre de 2023, dirigida al Dr. Mario Vílchez Madrigal, Director interino del Centro de Atención de Emergencias y Desastres (CAED), con respuesta recibida el 10 de noviembre de 2023.

- Entrevistas y reuniones con los siguientes funcionarios:

  - ✓ Máster Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones
  - ✓ El Dr. Mario Vílchez Madrigal, Director a.i del Centro de Atención de Emergencias y Desastres -CAED
  - ✓ Ing. Daniel Berrocal Zúñiga, jefe, Área Seguridad y Calidad Informática de la Dirección de Tecnologías de Información y Comunicaciones (DTIC).
  - ✓ Máster Doris Castillo Castillo, funcionaria de la Dirección de Sistemas Administrativos, Gerencia Administrativa.

MARCO NORMATIVO

- Ley General de Control Interno, No. 8292, julio 2002.
- Normas de Control Interno para el Sector Público de la Contraloría General de la República, febrero 2009.
- Normas Generales de Auditoría para el Sector Público, Resolución R-DC-064-2014, setiembre 2014.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
- Políticas Institucionales de Seguridad Informática, CCSS.
- Perfil funcional del Centro de Atención de Emergencias y Desastres (CAED), 2016.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría informa y previene al Jerarca y a los titulares subordinados acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37, 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"(…) Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)".*

ANTECEDENTES

El 31 de mayo de 2022, la CCSS detectó un ciberataque con impacto en toda la institución, resultando en la desconexión de los servicios tecnológicos a nivel nacional y afectando la continuidad de sus funciones.

Al respecto, la afectación se atribuye a la exposición de un virus tipo Ransomware (software malicioso diseñado para cifrar archivos del sistema y exigir un rescate a cambio de su liberación). Este tipo de amenaza suele tener un impacto sustancial en la integridad y disponibilidad de los datos, comprometiendo, en este caso específico, la operatividad de la Institución en materia de salud, pensiones y recaudación patronal.

Ante esta situación, el Ente Rector en Tecnologías de Información y Comunicaciones[1] recomendó de manera inmediata bloquear ciertos servicios TIC comprometidos y/o que requerían protección. En consecuencia, la identificación y contención de la amenaza, el análisis del incidente para comprender su alcance, la erradicación completa de la intrusión y la posterior recuperación, que incluye la restauración de las soluciones afectadas, formaron parte de las acciones esenciales para restablecer las condiciones normales de operación.

Con el fin de documentar ese avance, la DTIC emitió el "Informe de Cierre del Plan de Trabajo para la atención del ciberataque" suscrito por la Máster Idannia Mata Serrano, en ese momento Subgerente de la Dirección de Tecnologías de Información y Comunicaciones en oficio GG-DTIC-6373-2022 del 7 de noviembre de 2022, donde certifica la plena restauración de los sistemas de información y servicios tecnológicos en el ámbito que le corresponde a esa unidad.

En el informe supracitado se cita lo correspondiente a la articulación de esfuerzos realizados por la DTIC (acorde a las posibilidades y capacidad instalada de esa Dirección), a saber:

> *"(…) se consignaron esfuerzos conjuntos de esta Dirección y sus áreas adscritas en coordinación con otros actores institucionales en aras de habilitar tanto los servicios tecnológicos como garantizar razonablemente un marco de seguridad que permitiese minimizar los riesgos asociados a posibles acciones por parte de ciberdelincuentes, enfocada en la protección de la información y las buenas prácticas en esta materia.*
>
> *De acuerdo con lo establecido en la estrategia y el plan de trabajo que le acompañaba, con el compromiso de esta dirección, nos permitimos indicar que se atendieron cada una de las actividades y tareas señaladas en ambos documentos, con lo que a criterio de esta Dirección estaría cumplido el objetivo señalado en los citados documentos.*
>
> *En virtud de lo anterior, se remite para su información y consideración el Informe de Cierre de la Estrategia para el Restablecimiento de los Servicios Tecnológicos en la CCSS en su versión 1.0, el cual resultó de múltiples sesiones de trabajo, incluso muchas de ellas fuera de horario, las cuales consignamos, firmamos y anexamos."*

Además, el documento supra citado hace énfasis en la estrategia para la habilitación de los servicios, en relación con:

- Contención de la amenaza.
- Contratos de emergencia.
- Aseguramiento y recuperación de servicios críticos TIC.
- Aseguramiento y recuperación del parque tecnológico
- Recuperación de datos urgentes.

[1] La Dirección de Tecnologías de Información y Comunicaciones (DTIC) desempeña el papel de ente rector en el ámbito de Tecnologías de Información y Comunicaciones (TIC) en la Institución.

- Reforzamiento de la seguridad inicial; aseguramiento y recuperación de servicios TIC; habilitación y monitoreo; acciones de apoyo y control realizadas.

Finalmente, subraya la importancia de dar seguimiento a las mejoras propuestas en el Plan Reforzado de Ciberseguridad, en aras de aplicar las mejoras que corresponden al ámbito de Tecnologías de Información y Comunicaciones, al mencionar:

> *"Dándose por finalizada la atención de las actividades consideradas en el Plan establecido en la estrategia para la habilitación de servicios, se debe dar seguimiento a la atención del ciberataque desde una perspectiva de monitoreo, fortalecimiento y aseguramiento de los servicios tecnológicos. Para lo cual, desde la DTIC se continuará en el establecimiento del Plan de Fortalecimiento Proyecto Ciberseguridad, así como aplicación de mejoras y recomendaciones de entes externos para fortalecer la seguridad informática, continuidad en el aseguramiento de servidores y plataforma central, y demás actividades derivadas de la primera fase de atención del ciberataque que ha constituido la habilitación de los servicios institucionales.*
>
> *Por lo anterior es importante la conformación del gobierno de ciberseguridad por medio de un modelo institucional, la constante vigilancia y buenas prácticas que vayan mejorando la postura de ciberseguridad institucional, de ese modo lograr avanzar en los niveles de protección de la información y del resguardo del patrimonio institucional.*
>
> *Es importante indicar que la emergencia no ha finalizado. Se continúa trabajando para estabilizar la operación de los servicios y en el fortalecimiento de la seguridad informática, tarea que corresponde a toda la Institución"*

En este contexto, la CCSS logra restablecer las operaciones a la normalidad en los servicios TIC. No obstante, resulta igualmente crucial prevenir de manera razonable la materialización de riesgos futuros, no solo a nivel tecnológico, sino también en lo que concierne a las operaciones de negocio.

Sobre la respuesta, contingencia y continuidad a nivel de negocio y de las TIC

Una de las premisas fundamentales para cualquier organización es asegurar la continuidad institucional de los servicios que ofrece, independientemente de la presencia o ausencia de medios de comunicación digitales. Tal y como lo menciona la Contraloría General de la República, en el informe No. DFOE-EC-SGP-00001-2020 denominado *"Seguimiento de la gestión para la continuidad de los servicios públicos críticos ante la emergencia sanitaria, eje 1 gestión de la continuidad institucional"* refiriéndose a la identificación de las amenazas potenciales, los posibles impactos para las operaciones y los servicios públicos; y las medidas de protección y mitigación para que su afectación sea la mínima posible.

Dicha gestión tiene el propósito de asegurar razonablemente la prestación oportuna y de calidad de esos servicios, particularmente cuando se trata de procesos críticos[2] por su incidencia en el desarrollo social, económico y ambiental, en el bienestar y la protección de la vida, así como en el funcionamiento efectivo del aparato institucional.

Particularmente, la CCSS al llevar a cabo procesos críticos en salud, pensiones y recaudación patronal demanda la planificación de la gestión de continuidad del negocio para prevenir interrupciones en estas actividades sustantivas, ya sea por fallas eléctricas, financieras, tecnológicas o desastres naturales, entre otros eventos.

[2] Servicios públicos cuya interrupción resultaría en afectaciones altas o muy altas en el bienestar de la población y en el funcionamiento de las actividades socioeconómicas e institucionales del país

En ese contexto, las grandes organizaciones deben disponer de un Plan de Continuidad del Negocio (BCP)[3], aplicable a cualquier suceso que afecte los procesos críticos, independientemente de su vinculación con las tecnologías de información. La gestión de las unidades de servicio también evalúa medidas alternas durante incidencias, reconociendo la particularidad de cada situación.

Por ende, el BCP engloba planes de manera integral, como los de contingencia y de continuidad, incluyendo específicamente el correspondiente a las Tecnologías de la Información y Comunicaciones (TIC)[4], así como los de comunicación y recuperación, entre otros, todos revistiendo una importancia equiparable.

En lo que respecta al Plan de Continuidad de las TIC se estructura como una estrategia planificada con recursos y procedimientos particulares, orientados a obtener una restauración ordenada y eficiente de los sistemas de información debidamente alineados a los procesos críticos de la Institución. Este plan no se limita únicamente a la resolución técnica de problemas, ya que incorpora elementos de definición para evaluar el impacto y tolerancia ante la ausencia del funcionamiento de las aplicaciones informáticas.

En otras palabras, la continuidad del negocio (se centran en asegurar la operación general de la organización) y de las TIC (enfoca específicamente en mantener la funcionalidad de los servicios tecnológicos) son conceptos interrelacionados, es crucial reconocer que cada una posee sus propias diferencias y enfoques distintivos.

Iniciativas estratégicas gestionadas por la Institución en materia de continuidad del negocio

En el contexto de las iniciativas destinadas a generar un impacto significativo en la gestión de la continuidad de negocio, se identifica la siguiente:

- Dentro del marco de iniciativas relacionadas con el programa modelo de gobernanza de las Tecnologías de la Información y Comunicación (TIC)[5], se encuentra pendiente el desarrollo del proyecto que responde al nombre de " Habilitar la gestión de la continuidad de negocio", en línea con el siguiente **objetivo**:

  "Establecer un proceso que asegure la continuidad de las operaciones para los servicios críticos de la CCSS, manteniendo la información disponible a nivel aceptable para continuar con las operaciones de la Institución, ante cualquier escenario de desastre, que amenace la continuidad de sus operaciones."

En este contexto, las expectativas de la iniciativa se definieron de la siguiente manera:

- **Alcance**: La acción considera el desarrollo de una estrategia y un plan de continuidad de negocio que permita a la CCSS recuperar y operar sus servicios críticos ante la ocurrencia de un escenario de desastre. El Plan de Continuidad del Negocio incluye como parte de su estructura el Plan de Continuidad de TIC.
- **Plazo de ejecución para la iniciativa**: 18 meses.
- **Roles Responsables**: En calidad de administrador, la Dirección de Planificación Institucional asume un papel central. Las áreas involucradas abarcan la Dirección de Tecnologías de Información y Comunicaciones, todas las gerencias y todas las áreas de TIC.
- **Productos y entregables:** Implementación del proceso COBIT "DSS04 Gestionar la Continuidad"; Planes de Continuidad (de negocio y de TIC); Estrategia de entrenamiento para la continuidad de negocio; Informe de

[3] Un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés, Business Continuity Plan) es un conjunto de procesos y procedimientos diseñados para garantizar la operatividad y recuperación de una organización después de eventos disruptivos o desastres.

[4] Un Plan de Continuidad y Contingencia en Tecnologías de la Información y Comunicaciones (TIC) es un documento estratégico que establece las directrices y procedimientos para garantizar la disponibilidad, integridad y confidencialidad de los sistemas y servicios de información en situaciones adversas.

[5] La Gobernanza de las TI en la CCSS implica la estructura y procesos necesarios para tomar decisiones efectivas y supervisar las Tecnologías de la Información. En el 2018, la Institución recibió un informe detallando las brechas y las iniciativas requeridas para lograr este propósito. En el 2020 la Junta Directiva aceptó los resultados y dio instrucciones para avanzar en su implementación. Sin embargo, hasta la fecha, este programa ha enfrentado diversas limitaciones.

pruebas iniciales y resultados del Plan de Continuidad del Negocio; Informes de avance de la implementación del proceso.

Productos de Auditoría relacionados a la temática

Este Ente Fiscalizador a partir del 31 de mayo de 2022, momento en el cual fue conocido el ciberataque suscitado a la Caja Costarricense de Seguro Social, realizó informes de auditoría y otros productos asociados a los efectos de los ciberataques en la CCSS en aras de fiscalizar y asesorar a la Administración Activa sobre los principales procesos afectados por la desconexión de los sistemas de información y/o servicios tecnológicos, a saber:

Tabla No. 1
Productos emitidos en torno a la ciberseguridad de la CCSS
durante el 2022-2023

No. Producto	Asunto
AD-AATIC-063-2022	Oficio de Advertencia sobre gobierno y gestión de la ciberseguridad en la CCSS.
AD-AATIC-067-2022	Oficio de Advertencia sobre la exposición reciente a ataques cibernéticos a la CCSS.
AS-AATIC-072-2022	Oficio de Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.
AD-AATIC-074-2022	Oficio de Advertencia sobre equipos de laboratorio pertenecientes a los contratos de laboratorio (CAPRIS-ROCHE) afectados por el ciberataque del 31 de mayo del 2022.
AD-AATIC-078-2022	Oficio de Advertencia sobre la urgente necesidad de disponer de un sitio alterno de procesamiento de datos, dada la afectación sufrida en la prestación de servicios por el ciberataque del 31 de mayo de 2022.
AS-AATIC-087-2022	Oficio de Asesoría referente a la afectación en la gestión de Telesalud como resultado de los ataques cibernéticos ocurridos contra la Caja Costarricense de Seguro Social.
AS-AATIC-088-2022	Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico.
AS-AATIC-089-2022	Oficio de Asesoría en relación con acciones preventivas para minimizar la materialización de riesgos generados por eventuales debilidades en el Active Directory y servidores Exchange que permita la ejecución del ransomware “BlackCat”.
AS-AATIC-093-2022	Oficio de asesoría referente a las previsiones relacionadas con los contratos de prestación de servicios por terceros eventualmente afectados por el ciberataque sufrido el 31 de mayo de 2022.
AS-AATIC-101-2022	Oficio de asesoría en torno al cambio jerárquico del proceso Gestión de Tecnologías de Información y Comunicaciones propuesto en el oficio GG1067- 2022.
AS-AATIC-102-2022	Oficio de Asesoría en torno a los equipos tecnológicos utilizados para el Expediente Digital Único en Salud (EDUS) como parte de los contratos de servicios administrados suscritos entre la Caja Costarricense de Seguro Social (CCSS) y el Instituto Costarricense de Electricidad (ICE), afectados por el ciberataque del 31 de mayo del 2022.
AS-AATIC-103-2022	Oficio de asesoría referente a la instalación de una red WIFI en el Dirección General del hospital Guápiles, con la finalidad de acceder a servicios web externos como contingencia por el ciberataque sufrido el 31 de mayo de 2022.
AS-AATIC-107-2022	Oficio de Asesoría referente al tratamiento de los datos personales y medidas de seguridad.
AS-AATIC-108-2022	Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico.
AS-AATIC-112-2022	Oficio de Asesoría referente a la gestión del Consejo Tecnológico.

No. Producto	Asunto
AS-AATIC-113-2022	Oficio de Asesoría sobre el restablecimiento en la operación de sistemas de información y bases de datos.
AS-AATIC-114-2022	Oficio de Asesoría referente al uso de WhatsApp para el envío y recepción de información institucional.
AS-AATIC-116-2022	Oficio de Asesoría referente a los Planes de Continuidad de TIC.
AS-AATIC-122-2022	Oficio asesoría referente a las acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta “Log4J”.
AS-AATIC-124-2022	Oficio de Asesoría en relación con riesgos identificados en materia de protección de datos por la implementación de mecanismos contingentes en la atención de pacientes.
AS-AATIC-125-2022	Oficio de Asesoría sobre el comportamiento, tácticas y herramientas utilizadas por los ciber atacantes.
AS-AATIC-127-2022	Oficio de Asesoría sobre la actualización del software y la infraestructura en TIC
AS-AATIC-130-2022	Oficio de asesoría referente a la gestión del Directorio Activo
AS-AATIC-131-2022	Oficio de Asesoría referente soluciones de autenticación en sistemas informáticos.
AS-AATIC-135-2022	Oficio de Asesoría sobre el impacto en la prestación de servicios y medidas de contingencia, producto del ataque cibernético en la plataforma tecnológica institucional.
AS-AATIC-137-2022	Oficio de Asesoría relacionado con la gestión de Bases de Datos y sus mecanismos de seguridad.
AS-AATIC-138-2022	Oficio de Asesoría referente al uso de servicio de internet (MIFI) en la Dirección de Inspección como contingencia al ataque cibernético sufrido el 31 de mayo de 2022.
AS-AATIC-146-2022	Oficio de Asesoría referente al procedimiento de registro y pago de incapacidades descrito en el oficio GF-0410-06-2022/GM-8071-2022 del 5 de julio del 2022.
AS-AATIC-147-2022	Oficio de asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social
AS-AATIC-152-2022	Oficio Asesoría referente al establecimiento de una hoja de ruta para brindar seguimiento a las recomendaciones emitidas por Deloitte, GBM, Microsoft y el Centro Criptológico Nacional posterior al análisis e investigación del incidente suscitado el 31 de mayo del 2022.
AS-AATIC-155-2022	Oficio de asesoría relacionado con amenazas generadas por el ransomware DeadBolt que afecta los almacenamientos en dispositivos NAS.
AS-AATIC-167-2022	Oficio de Asesoría sobre la importancia de establecer una estrategia integral que promueva la formación, capacitación y concientización en seguridad informática, seguridad de la información y ciberseguridad.
AS-AATIC-168-2022	Oficio de Asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento.
AS-AATIC-169-2022	Oficio de Asesoría sobre la gestión de ciberseguridad en el uso de dispositivos móviles.
AS-AATIC-174-2022	Oficio de Asesoría sobre ciberseguridad hospitalaria.
AS-AATIC-175-2022	Oficio de Asesoría relacionado con los Sistemas de Gestión de Privacidad de la Información en el contexto actual de la Caja Costarricense de Seguro Social.
AS-AATIC-177-2022	Oficio de Asesoría sobre la gestión de servicios de computación en la nube como mecanismo de contingencia.
AS-AATIC-182-2022	Oficio de Asesoría Referente a Nuevas Vulnerabilidades Explotadas Activamente que han sido incorporadas al Catálogo de Vulnerabilidades Conocidas.
AS-AATIC-183-2022	Oficio de Asesoría relacionado a la gestión e implementación de la herramienta MicroCLAUDIA en el contexto del Ciberataque a la CCSS.
AS-AATIC-184-2022	Oficio de Asesoría sobre la importancia del desarrollo seguro de sistemas y aplicaciones institucionales.
AS-AATIC-185-2022	Oficio de Asesoría relacionado con los riesgos detectados en materia de Seguridad de la Información y Ciberseguridad en instrumento elaborado por la Contraloría General de la República.

No. Producto	Asunto
AS-AATIC-186-2022	Oficio de Asesoría Referente a Aplicaciones que Originan Descargas de Malware.
AS-AATIC-190-2022	Oficio de Asesoría sobre las capacidades asociadas con la gestión de incidentes de ciberseguridad.
AS-AATIC-194-2022	Oficio de Asesoría referente al sitio alterno de procesamiento de datos de la Gerencia de Pensiones, dada la afectación sufrida en la prestación de servicios por el ciberataque del 31 de mayo de 2022.
AS-AATIC-198-2022	Oficio de Asesoría sobre ciberseguridad para dispositivos y equipos médicos.
AS-ATIC-006-2023	Oficio de Asesoría relacionado con la necesidad de brindar seguimiento a los productos de auditoría emitidos en torno al ciberataque a la Institución que llevó a la desconexión de servicios tecnológicos el 31 de mayo del 2022.
AI-865-2022	Sobre Oficio de Advertencia AD-AATIC-067-2022 referente a exposición reciente a ataques cibernéticos a la CCSS.
AI-884-2022	Oficio de información en relación con el acceso a la página Web de la Biblioteca Nacional de Salud y Seguridad Social (BINASSS) en el contexto de los ataques cibernéticos a la CCSS.
AI-905-2022	Oficio de información en relación con acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta “Mimikatz”.
AI-1043-2022	Oficio de información relacionado con el riesgo de ransomware detectado en la plataforma de Microsoft 365.
AS-AAFP-073-2022	Oficio de Asesoría sobre el proceso de inversiones del Régimen de IVM ante el ataque cibernético sufrido por la CCSS el 31 de mayo del 2022.
AS-AAFP-076-2022	Oficio de Asesoría referente a las acciones de contingencia consideradas por el Fondo de. Retiro de Empleados ante la situación provocada por el ciberataque a la CCSS, el 31 de mayo del 2022.
AS-AAFP-077-2022	Oficio de Asesoría sobre las medidas contingentes adoptadas para mantener continuidad en los procesos liderados por la Dirección de Coberturas Especiales ante el ataque cibernético sufrido por la CCSS, el 31 de mayo del 2022.
AS-AAFP-080-2022	Oficio de Asesoría sobre el proceso de cobro de Créditos Hipotecarios ante el ataque cibernético sufrido por la CCSS el 31 de mayo del 2022.
AS-AAFP-120-2022	Oficio de asesoría sobre medidas de contingencia para la gestión de Ingresos y Egresos en la Plataforma de Cajas Institucional ante el ataque cibernético sufrido por la C.C.S.S. el 31 de mayo 2022.
AS-AAFP-156-2022	Oficio de Asesoría sobre la facturación de servicios asociados a las tarifas mensuales diferenciadas que se generan para 29 Hospitales y 10 Áreas de Salud.
AS-AAFP-163-2022	Oficio de Asesoría sobre alternativa de contratación de seguro para mejorar la ciberseguridad a nivel Institucional.
AD-AAO-061-2022	Oficio de Advertencia referente a la continuidad de la prestación de servicios en la Sucursal de Upala.
AS-AAO-067-2022	Oficio de asesoría referente a la afectación en la gestión de recursos humanos como resultado de los ataques cibernéticos ocurridos contra la Caja Costarricense de Seguro Social.
AS-AAO-081-2022	Asesoría sobre principales riesgos estratégicos en los procesos de dirección relacionados con la oportunidad de los pagos salariales a los funcionarios de la Caja Costarricense de seguro Social.
AS-AAO-092-2022	Oficio de asesoría referente a las disposiciones emitidas en los oficios GG-DAGP-0823-2022 y GG-DAGP-0831-2022, relacionados con las medidas de contingencia transitorias en materia de gestión de recursos humanos, producto del ciberataque contra la institución.
AS-AAO-121-2022	Oficio de asesoría referente a la afectación en los servicios de ingeniería y mantenimiento producto del ataque cibernético del 31 de mayo de 2022.

No. Producto	Asunto
AS-AAO-136-2022	Oficio de asesoría referente a la afectación en la gestión de contratación administrativa, abastecimiento de bienes y servicios en Centros de Salud, producto del ataque cibernético del 31 de mayo de 2022.
AS-AAO-140-2022	Asesoría sobre principales riesgos estratégicos en los procesos de dirección relacionados con la gestión de la Dirección Jurídica.
AS-AAO-141-2022	Oficio de asesoría referente a la gestión de la administración del riesgo en el Programa de Equidad de Género en el contexto del ciberataque a la CCSS.
AS-AAO-142-2022	Asesoría en relación con la cultura institucional de administración del riesgo y el proceso de simplificación de trámites y mejora regulatoria, en el contexto del ciberataque suscitado en la CCSS el 31 de mayo 2022.
AS-AAO-143-2022	Oficio de asesoría referente a la gestión de la administración del riesgo en la Dirección de Bienestar Laboral en el contexto del ciberataque a la CCSS.
AS-AAO-149-2022	Oficio de asesoría referente a la afectación generada a los procesos sustantivos de la Dirección de Comunicación Organizacional debido al ataque cibernético en la CCSS.
AS-AAO-151-2022	Oficio de asesoría referente a la afectación generada a los procesos sustantivos de la Dirección de Planificación Institucional debido al ataque cibernético en la CCSS.
AD-AAS-062-2022	Oficio de Advertencia sobre la gestión de la continuidad de la prestación de servicios en la Institución ante emergencias o desastres.
AS-AAS-095-2022	Oficio de Asesoría sobre la gestión de la prescripción, despacho y custodia de medicamentos en los servicios de salud ante el ciberataque que sufrió la institución.
AS-AAS-117-2022	Oficio de asesoría referente a las acciones a impulsar para garantizar la continuidad de los servicios de Laboratorio Clínico ante los riesgos generados por el ataque cibernético en la institución.
AS-AAS-118-2022	Oficio de Asesoría referente a las estrategias orientadas en la continuidad de servicios para la atención de la pandemia contra la enfermedad COVID19, ante el escenario originado por el hackeo institucional de los sistemas institucionales.
AS-AAS-123-2022	Oficio de Asesoría sobre la gestión de captación, análisis, distribución, trazabilidad y custodia de los hemo componentes ante el ciberataque.
AS-AAS-126-2022	Oficio de Asesoría sobre la gestión en los servicios de cirugía ante el ciberataque que sufrió la institución.
AS-AAS-132-2022	Oficio de Asesoría sobre la gestión en los servicios de radiología e imágenes médicas ante el ciberataque que sufrió la Institución.
AS-AAS-145-2022	Oficio de asesoría sobre la gestión en los servicios de anatomía patológica ante el ciberataque que sufrió la Institución.
AS-AAS-153-2022	Oficio de Asesoría sobre la prestación de servicios de salud en la Consulta Externa, ante el hackeo a los sistemas de información institucionales.
AS-AAS-154-2022	Oficio de Asesoría referente a riesgos en el funcionamiento y continuidad de los servicios de Farmacia ante el ataque cibernético en la institución.
AS-AAS-170-2022	Oficio de Asesoría referente a la gestión de las agendas médicas en la Consulta Externa Especializada del Hospital San Juan de Dios.

Fuente: elaboración propia, a partir de la información extraída del SIGA SAGAL el 31-07-2023.

Todo lo anterior, definido en apoyo a la identificación de aspectos relevantes que permitiera asesorar y advertir bajo una modalidad ágil que permitiera brindar a la Administración insumos de mejores prácticas y observaciones a las cuales dar prioridad en medio de la atención de la emergencia.

HALLAZGOS

1. SOBRE EL AVANCE DE INICIATIVA "HABILITAR LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO" VINCULADA AL PROGRAMA DE GOBERNANZA Y GESTIÓN DE LAS TIC

Este Órgano Fiscalizador observó que la iniciativa presentada por la empresa PriceWaterhouseCoopers (PwC) en 2018, bajo el título "Habilitar la gestión de la continuidad del negocio" y oficializada como uno de los objetivos del Programa de Gobernanza y Gestión TIC, aún no ha sido iniciada[6]. Adicionalmente, es importante señalar que hasta el momento no se ha realizado una asignación formal de un coordinador y/o administrador del proyecto de marras.

En este sentido, la falta de avances en la iniciativa a lo largo de los últimos cinco años preocupa a esta Auditoría, ya que no se han presentado propuestas concretas para implementar mejoras, tanto en las competencias del negocio, como en las Tecnologías de la Información y Comunicación (TIC). La finalidad de lo anterior es minimizar en la mayor medida posible cualquier impacto derivado de posibles incidentes o interrupciones que podrían comprometer la operación de los procesos críticos y los servicios tecnológicos. En otras palabras, se busca preservar la disponibilidad de información a un nivel aceptable, lo cual se considera imperativo, especialmente después de la ocurrencia de eventos como el ciberataque perpetrado en la CCSS.

Según el documento suministrado a la CCSS, como producto de la fase de "Analizar las brechas integral del Gobierno de las Tecnologías de Información y Comunicaciones evaluando el Gobierno de la Seguridad de la Información" del Proyecto Servicios de consultoría para el Diseño de Modelo de Gobernanza de las TIC y horas de servicio por demanda para el desarrollo del Plan de Intervención Inmediata (Contrato No.007-2016 correspondiente a la Licitación Abreviada No.2016LA-000003-1150), las debilidades que motivaron la necesidad de plantear la iniciativa supracitada fueron:

Tabla No. 2
Identificación y análisis de hallazgos / brechas
con respecto al proceso Gestionar la continuidad, 2017

Proceso	Hallazgo	Brecha
DSS04 Gestionar la continuidad	No existen mecanismos que permitan identificar claramente cuáles son los procesos de negocio que son críticos para la institución y cuáles son los procesos y servicios de TIC que los apoyan.	Establecer una figura dentro del ámbito institucional de la CCSS, responsable de garantizar la continuidad de las operaciones y servicios brindados por la institución. Apoyado por una contraparte TIC responsable de garantizar la continuidad en las soluciones y servicios tecnológicos.
	No existen políticas, roles, responsables, requerimientos y acuerdos relacionados a la continuidad de las operaciones de negocio soportadas en servicios y soluciones TIC.	Garantizar que la gestión de continuidad es considerada de manera integral dentro de la gestión institucional de riesgos.
	No existe un proceso que apoye la gestión de riesgos relacionada con la continuidad de las operaciones de TIC.	Desarrollar un ejercicio de análisis de los impactos del negocio que permita a la CCSS identificar los procesos críticos de la institución.
	Existes iniciativas documentadas e implementadas que buscan la definición de un plan de continuidad dentro de las diferentes unidades de TIC de la institución, sin	Documentar e implementar procesos formales estándar de uso institucional que

[6] Según el informe GG-DTIC-2488-2023 fechado el 25 de abril de 2023, el proyecto permanecía en estado "Pendiente". En el informe GA-DTIC-4823-2023 del 27 de julio de 2023, se menciona que la iniciativa está catalogada como "Pendiente de diseñar e implementar". En relación con el informe GG-DTIC-7789-2023 del 21 de noviembre de 2023, el estado de la iniciativa se mantiene en un 0%.

Proceso	Hallazgo	Brecha
	embargo no existen mecanismos formales que permitan garantizar la idoneidad, efectividad y apego a las buenas prácticas de cada uno de los planes desarrollados, así como no existe garantía de que se aplique un enfoque integral que aborde los procesos críticos de la institución soportados por servicios y soluciones TIC.	apoyen la gestión de la continuidad institucionales de manera integral considerando los procesos y soluciones de negocio, y los servicios y soluciones TIC.
	Existe una iniciativa en curso para la habilitación de un centro de recuperación ante desastres bajo la modalidad de aprovisionamiento por demanda, la cual se enfoca en los principales servicios institucionales prestados por la DTIC	Documentar e implementar procedimientos formales estándar de uso institucional para la gestión de la contingencia y la continuidad de los servicios TIC.
	No existe un plan institucional de continuidad de operaciones y servicios que garantice la operatividad de la organización en caso de eventos disruptivos.	
	Dentro de los términos contractuales de contratación a proveedores se incluyen directrices que buscan garantizar la disponibilidad del servicio, sin embargo no se aborda de manera conjunta la definición de un plan de continuidad en caso de eventos disruptivos.	
	No existen mecanismos formales de ámbito institucional que garanticen la comunicación, la transferencia de conocimiento y la formación de los funcionarios sobre las medidas y procedimientos de continuidad, y su participación en el desarrollo de las mismas.	
	No existe una definición clara de los responsables y las acciones a ejecutar como respuesta a incidentes de continuidad.	

Fuente: Entregable “Análisis integral de brechas”, pwc, diciembre 2017

En línea con lo anterior, los aspectos abordados por la empresa consultora resaltan la oportunidad de mejora relacionada con una gestión eficaz de la continuidad. Este planteamiento se intensifica a partir del ciberataque experimentado por la Institución en mayo de 2022, subrayando con urgencia la necesidad imperante de fortalecer procesos y actividades en diversas áreas, tanto a nivel de negocio como tecnológico.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021, en el apartado “Procesos del marco de Gestión de TI”, establece en relación con la “Planificacion Tecnológica Institucional”, lo siguiente:

> *“La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público. Adicionalmente, que incorpore indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia.”*

Además, en ese mismo marco normativo, en el apartado “Procesos del marco de Gestión de TI”, se establece lo correspondiente a la “Gestión de Proyectos que implementan recursos tecnológicos”:

> *“La institución debe gestionar los proyectos que permitan habilitar sus iniciativas para el logro de los objetivos estratégicos, satisfaciendo los requerimientos y en cumplimiento con términos de calidad, tiempo, presupuesto y uso óptimo de los recursos, de acuerdo con las buenas prácticas y estándares preestablecidos.*

La Unidad de TI debe establecer el portafolio de proyectos debidamente priorizados, identificando en cada iniciativa el beneficio a generar por la habilitación de tecnologías de información. Su administración a través de la ejecución de los planes asociados, deben permitir obtener el resultado esperado, minimizando el riesgo asociado a eventos durante la ejecución del proyecto y garantizando la calidad y la entrega de valor para el logro de los objetivos institucionales.

La Unidad de TI debe establecer un modelo estandarizado para la gestion y administración de proyectos de perfil tecnológico, así como su continua actualización, divulgación y capacitación a funcionarios."

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002, en su apartado 8.5 establece que:

"7.4 El Consejo Tecnológico es el responsable de asegurar la generación de valor y el logro de los beneficios de las inversiones en TIC, lo cual se verificará tanto durante la ejecución de la inversión como una vez implementada en su totalidad.

La definición del valor y beneficios de los proyectos e inversiones en TIC se llevará a cabo desde su planteamiento inicial, por medio de caso de negocio, siendo estos considerados como elementos clave para el análisis, priorización y aprobación por parte del Consejo Tecnológico.

El valor y beneficios de cada inversión en TIC se definirán de forma clara y concreta, utilizando elementos cuantificables que faciliten el monitoreo y verificación de la generación de valor y el logro de los beneficios, tanto durante la ejecución de la inversión como posterior a su conclusión."

Asimismo, esa misma Directriz, en su apartado 8.5 "El Consejo Tecnológico es el responsable de asegurar la generación de valor y el logro de los beneficios de las inversiones en TIC, lo cual se verificará tanto durante la ejecución de la inversión como una vez implementada en su totalidad", establece:

"7.4 El control y seguimiento a la implementación de la estrategia tecnológica contemplará el desempeño y los riesgos asociados con la gestión de TIC de la CCSS

Las actividades de control de la implementación de la estrategia permiten detectar tempranamente posibles desviaciones en el logro de los objetivos, el control interno y las condiciones del entorno que puedan afectar el rendimiento de TIC. Es responsabilidad de la DTIC llevar a cabo las acciones necesarias para el logro de la estrategia tecnológica, así como del Consejo Tecnológico brindar patrocinio y dar seguimiento por la alineación de los resultados de estas con la estrategia institucional."

Considerando que la iniciativa no ha iniciado su implementación pese a su conceptualización desde el 2018, se toma como referencia el "análisis estratégico del programa de gobernanza y gestión de las TICS y propuesta de fortalecimiento para la ejecución de las iniciativas" suscrito por el Lic. Josué Zúñiga Hernández, en su momento Asesor de la Gerencia General, remitido mediante oficio GG-2205-2022 del 19 de agosto del 2022, suscrito por el Dr. Roberto Cervantes Barrantes, Gerente General, en el cual señala limitaciones en el desarrollo de las iniciativas, sin ser el proyecto "Habilitar la gestión de la continuidad del negocio" la excepción:

"El proceso de adopción de las sanas prácticas insertas en el Cobit, debe gestionarse de forma holística de manera que se garantice el involucramiento de la alta gerencia, los giros de negocio, y el componente tecnológico de la institución, sin embargo, el diseño y desarrollo del modelo de gobernanza y gestión de las tic se ha concentrado en la Dirección de Tecnologías de Información y Comunicaciones, más que todo por aspectos de cultura organizacional y no por elementos técnicos, fundamentados y justificados.

Es necesaria la participación de los giros de negocio para la adecuada adopción de un modelo de Gobierno basado en las sanas prácticas del Cobit, razón por la cual se considera que el habilitar el Consejo

Tecnológico para ese fin, fue un acierto de la Junta Directiva, no obstante, como ya se evidenció ese ente colegiado no ha asumido la responsabilidad que ese ente decisor le asignó.

Los dos hitos, antes mencionados, pueden considerarse como las principales causas del avance registrado para el Programa de Gobernanza y Gestión de las TIC, toda vez, que la DTIC se ha visto limitada en recursos, y capacidad para afrontar el esfuerzo que requiere una iniciativa de esta envergadura, asimismo, la separación entre el proceso de negocio y la parte técnica ha generado que los productos en ejecución estén asociados a características de índole técnico o con poca consideración de las necesidades de la organización.

Esas situaciones han motivado que un programa conformado con 29 iniciativas, y con 6 años de haber iniciado registre únicamente 4 proyectos finalizados, entre otros aspectos."

En relación con este asunto, la empresa consultora PWC emitió oficio sin número del 1 de junio de 2023, dirigido a la Máster Vilma Campos Gómez, Gerente Administrativa, con el propósito de informarle sobre los principales desafíos y retos del Programa asociado con los "Servicios profesionales de consultoría para acompañamiento en la implementación del Modelo de Gobernanza y Gestión de las TIC en la CCSS. Licitación pública 2019LN-000001-1150", citando:

"(…) tomando en cuenta el estado actual del Programa, así como las dificultades y retos que se han enfrentado, producto de factores de índole interna asociados con constantes cambios estructurales, así como cambios periódicos en la visión de los altos mandos de la Institución, aunado a situaciones externas a las cuales ha tenido que hacer frente la CCSS, como es el caso de la atención de la Pandemia COVID-19, el ciberataque sufrido en mayo del 2022, entre otros; consideramos de valor hacer un recuento del trabajo realizado, así como de las principales situaciones que visualizamos han afectado el logro de los objetivos establecidos a lo largo de los primeros tres años de contratación, las cuales consideramos serán de valor tomar en cuenta para establecer las iniciativas en las cuales se estarán orientando las acciones prioritarias durante este cuarto y último año de servicio (el cual se encuentra en activo y sin ejecución desde el pasado mes de febrero, donde restan únicamente 9 meses para su culminación), en pro de garantizar el aprovechamiento de los recursos disponibles para el contrato, la ocupación efectiva de nuestros recursos y la provisión del máximo valor para la Institución."

En este contexto, las significativas demoras en la ejecución de las medidas destinadas a preservar la integridad y estabilidad operativa de la institución frente a posibles eventos podrían dar lugar a desatender recomendaciones clave, así como exponer a la CCSS a riesgos que se traducen en la materialización de vulnerabilidades ante un nuevo ciberataque, desastre natural o cualquier otro evento que cause interrupción de servicios institucionales.

2. SOBRE EL PLAN DE CONTINUIDAD DEL NEGOCIO Y EL PLAN DE RECUPERACIÓN ANTE DESASTRES

Se constató que antes de la materialización del ciberataque ocurrido en mayo de 2022, la institución carecía de un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), con enfoque multiamenaza y de cobertura institucional (integral y/o consolidado).

A modo de ejemplo, se citan algunas de las acciones llevadas a cabo en forma posterior por la Gerencia Médica, con el objetivo de proporcionar orientación sobre las medidas de contingencia a considerar por parte de los centros médicos, a saber:

- GM-7133-2022 del 4 de junio del 2022 donde se especifica a las unidades a cargo de la Gerencia Médica las acciones de contingencia para los servicios de redes ante las medidas preventivas relacionadas con los sistemas de información institucionales.
- GM-8015-2022 del 5 de julio del 2022 especificando las acciones de contingencia para la gestión del informe estadístico mensual (IEM) al conjunto de unidades a cargo de la Gerencia Médica.

- GM-8793-2022 del 5 de julio del 2022 especificando las “Acciones de contingencia para la gestión del informe estadístico mensual (IEM) - versión 2” al conjunto de unidades a cargo de la Gerencia Médica.
- GM-8116-2022 del 6 de julio del 2022, con el asunto estrategias para la continuidad en la captación de información listas de espera y programación quirúrgica, dirigido a las unidades que tiene a cargo la Gerencia Médica.

Esto evidencia la falta de un plan previo con el detalle de todas las recomendaciones antes mencionadas y que, en caso de materializarse eventos específicos en los cuales se afecte la continuidad de los servicios, este pueda ser implementado.

Es decir, a pesar de los eventos significativos como la pandemia por COVID-19 y el mencionado ciberataque, hasta la fecha, la CCSS no se han elaborado planes integrales como el BCP o DRP. Aunque existen documentos específicos para abordar la continuidad o contingencia de eventos particulares, tal como se refleja en el "Plan Contingencial para la Atención de la Emergencia ante el Ciberataque (PCAEC)" y el "Plan para la Adaptación y Recuperación de Servicios ante la Pandemia por COVID-19", ambos emitidos posterior a la declaración de la emergencia respectiva.

En ese orden de ideas, resalta la falta de normativa, estrategias e instrucciones sobre la necesidad de garantizar la continuidad de los servicios ofrecidos por la CCSS a nivel operativo y no únicamente en lo que refiere a TIC (de ser así dejaría una brecha en la preparación para afrontar otro tipo de eventos diversos), fundamentado en los principios propuestos por las mejores prácticas, tales como las normas ISO 22301[7], INTE G-130[8] o consideraciones relacionadas con la gestión de riesgos.

Las Normas de Control Interno para el Sector Público, en el Capítulo IV: Normas sobre actividades de control, en el apartado 4.2 Requisitos de las actividades de control, cita:

> *“Respuesta a riesgos. Las actividades de control deben ser congruentes con los riesgos que se pretende administrar, lo que conlleva su dinamismo de acuerdo con el comportamiento de esos riesgos.”*

En ese mismo marco normativo, el Capítulo IV: Normas sobre actividades de control, en el apartado 4.3 Protección y conservación del patrimonio, menciona:

> *“El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales activos y los riesgos relevantes a los cuales puedan verse expuestos, así como los requisitos indicados en la norma 4.2”*

Finalmente, ese mismo marco normativo, el Capítulo V: Normas sobre sistemas de información, en el apartado 5.4 Gestión documental, a saber:

> *“El jerarca y los titulares subordinados, según sus competencias deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.”*

[7] La ISO 22301 es una norma global que guía a las organizaciones en la creación y gestión de sistemas para garantizar la continuidad del negocio, abordando la identificación y respuesta a riesgos, y asegurando la operación continua frente a interrupciones.
[8] Norma que apoya la implementación de Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro-Requisitos y orientación para su uso.

El Plan Estratégico Institucional 2023-2033, en el capítulo 7. Temas Trasversales, cita en lo correspondiente a la "Gestión de riesgos":

> *La Caja Costarricense de Seguro Social mediante la gestión integral de riesgos brindará en todos los niveles organizacionales información relevante y actualizada para la toma de decisiones, por medio del establecimiento de un marco general para la gestión integral de riesgos como elemento transversal al quehacer institucional, promoviendo la cultura de gestión de riesgos, encauzando a la Institución al cumplimiento de sus objetivos, al aseguramiento en la continuidad de los servicios, la sostenibilidad y la mejora continua.*

Además, en ese mismo capítulo pero refiriéndose al tema de "prevención y atención de emergencias y desastres", menciona lo siguiente:

> *La Caja Costarricense de Seguro Social contará con un modelo de gestión de emergencias y desastres ante eventos disruptivos, que parte del análisis de las amenazas, las experiencias pasadas y la generación de escenarios de riesgo de desastres, para contar con acciones que permitan la continuidad de los servicios, antes, durante y después de un hecho que pueda poner en riesgo la prestación de los servicios. Desarrollará actividades, normativa y lineamientos tendientes a la reducción del riesgo de desastre en todos los ámbitos institucionales, así como el aumento de la capacidad de adaptación y reconversión necesarias desde las etapas previas de preparación hasta la respuesta institucional.*
>
> *Para ello fortalecerá la capacidad de gestión ante las emergencias y desastres, de manera articulada, que con información fidedigna y oportuna le permitan la toma de decisiones y la atención de la población afectada con un uso adecuado y eficaz de los recursos institucionales.*

El Dr. Mario Vílchez Madrigal, quien ocupa el cargo de Director en funciones en el Centro de Atención de Emergencias y Desastres (CAED), indicó:

> *"El CAED, a partir de la atención de la emergencia por COVID, ha gestionado una serie de acciones para poder atender las necesidades de la Institución, que, con el paso del tiempo, son diferentes y requieren un CAED más fortalecido y con un enfoque multi amenaza. Esto forma parte de las lecciones aprendidas que como unidad se han externado y la visión que se tiene de ella. De manera que, con un corte de mayor liderazgo y estrategia, se solicitó en meses anteriores, la actualización del modelo de gestión de esta Unidad a la Dirección de Sistemas Administrativos, asimismo, el plan de gobernanza que acompaña la propuesta de abordaje. Aunado a lo anterior, se trabaja en la generación de guías, manuales y capacitaciones que permitan una preparación y atención de emergencias mejor direccionada y con unas capacidades institucionales mayores. En esa línea ya nos encontramos en la ruta de la implementación de la norma INTE/ G-130 publicada este año, para planes de continuidad en servicios públicos. Las principales limitantes han estado en la línea de la capacidad de respuesta que tiene el CAED como unidad, en el alcance (que ya se está modificando en el modelo) y en recurso humano. Con base en eso, los retos de la unidad a futuro se definen en la línea de una mejor institucionalización de los preparativos y atención de emergencias provocadas por eventos de alto impacto para la continuidad de servicios institucionales críticos o priorizados (siendo que se trata de algo diferente a la continuidad en tiempos ordinarios), la aprobación del nuevo modelo y la aprobación del plan de gobernanza para su correcta implementación."*

Además, la situación evidenciada podría ser la causa del avance disminuido que experimentan las iniciativas planteadas en la institución para habilitar la gestión de la continuidad del negocio. Esto, a su vez, afecta el conjunto de acciones relacionadas con la concientización, el desarrollo de labores, entrega de productos finales, entre otros aspectos interrelacionados a la temática de marras.

En ese sentido, la ausencia de integración del BCP y DRP, expone a la CCSS a riesgos significativos y efectos perjudiciales ante la exposición a eventos que ocasionen crisis o emergencias; esto debido a la falta de un plan

estructurado alineado para mitigar la pérdida de datos críticos, interrupciones prolongadas en las operaciones, daño a la reputación y, en última instancia, un impacto financiero negativo.

En otras palabras, la carencia de enfoque integral para gestionar y recuperarse de eventos disruptivos deja a la institución vulnerable frente a una amplia gama de amenazas, aumentando la probabilidad de pérdidas severas y dificultando la capacidad de recuperación eficiente.

3. VALORACIONES INTEGRALES Y ESTANDARIZADAS SOBRE LA AFECTACIÓN EN LOS PROCESOS INSTITUCIONALES

Se constató la ausencia de valoraciones integrales, estandarizadas y/o de conocimiento por el nivel estratégico de la institución (Junta Directiva, Presidencia, Consejo tecnológico y Cuerpo Gerencial) en la cual se evidencie la cuantificación del impacto en diversas áreas, como las reputacionales, operativas, cumplimiento normativo, productividad de los empleados, utilización de seguros y/o pólizas, entre otros aspectos interrelacionados al abordaje de la emergencia vinculada con el ciberataque experimentado por la Caja Costarricense de Seguro Social en mayo del 2022.

En ese sentido, los únicos informes observados por esta Auditoría Interna fue el desarrollado por la Dirección de Tecnologías de Información y Comunicaciones "Estrategia para el Restablecimiento de los Servicios Tecnológicos en la CCSS, Informe de Cierre, Versión 1.0" dado a conocer mediante oficio GG-DTIC-6373-2022 del 7 de noviembre del 2022; “Informe referente al impacto financiero por ciberataque” comunicado mediante oficio GF-1388-2023 del 14 de abril del 2023; “Informe referente a la determinación del impacto financiero generado por el ciberataque del 31 mayo 2022” detallado en oficio GF-2171-2023 del 12 de junio 2023; y el “Informe de situación actual, Gerencia de Pensiones, Planes de contingencia aplicados para la continuidad de los servicios.” remitido por la Gerencia de Pensiones mediante oficio GP-945-2022 del 10 de junio del 2022. No obstante, estos informes carecen de uniformidad en cuanto al tipo de análisis realizado y, eventualmente, en el nivel de detalle y especificación, lo que impide su estandarización y evidencia la oportunidad de mejora.

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el inciso 6.2 “Orientaciones para el seguimiento del SCI” indica:

> *“El jerarca y los titulares subordinados, según sus competencias, deben definir las estrategias y los mecanismos necesarios para el efectivo funcionamiento del componente de seguimiento del SCI. Dichas orientaciones deben ser congruentes y estar integradas a las gestiones relacionadas con la operación, mantenimiento y perfeccionamiento del SCI, ser de conocimiento de todos los funcionarios, estar disponibles para su consulta y ser revisadas y actualizadas periódicamente.*
>
> *Como parte de tales orientaciones, entre otros, se deben establecer formalmente, mecanismos y canales de comunicación que permitan la detección oportuna de deficiencias y desviaciones del SCI, y que quienes las detecten informen con prontitud a la autoridad competente para emprender las acciones preventivas o correctivas que procedan, de acuerdo con la importancia y riesgos asociados.”*

El perfil funcional del Centro de Atención de Emergencias y Desastres (CAED) publicado en el 2016, refiere en cuanto funciones sustantivas de la unidad, lo siguiente:

> *“- Asesorar a las diversas instancias institucionales (Consejo de Presidencia y Gerentes, Directores Regionales, Directores de Hospitales y Áreas de Salud, entre otros), para orientar técnicamente las decisiones en la preparación, respuesta y recuperación en caso de emergencias o desastres y facilitar la continuidad de los servicios.*
>
> *- Asesorar a los Comités de nivel central, regional y local en la formulación y ejecución de los planes y estrategias a desarrollar, ante la ocurrencia de emergencias o desastres, o provocados por el hombre, con*

la finalidad de contar con los instrumentos que permitan atender eficazmente cualquier evento de esta naturaleza."

El Dr. Mario Vílchez Madrigal, quien ocupa el cargo de Director en funciones en el Centro de Atención de Emergencias y Desastres (CAED), refiriéndose a la generación de un marco de referencia institucional y debidamente estandarizado, indicó:

"(…) estamos apuntando a la implementación de la norma INTE/ G-130 para generar ese marco de referencia institucional, de corte muy estratégico, para que cada dueño de negocio pueda desarrollar los planes de continuidad específico en una forma estandarizada, teniendo claridad de cuáles son los procesos y actividades críticas priorizadas a nivel institucional, y no solo las actividades de su propio negocio."

La falta de este tipo de evaluaciones dificulta la comprensión integral de la medición precisa del nivel de afectación del evento y sus consecuencias, ya que el grupo de involucrados en la toma de decisiones carecen de un análisis sintetizado y con las perspectivas especializadas, entre otras áreas trascendentales.

Asimismo, esa condición impide la identificación estratégica de oportunidades de mejora y obstaculiza la generación de lecciones aprendidas esenciales para fortalecer la resiliencia de la organización frente a futuros eventos similares.

4. SOBRE EL FORTALECIMIENTO DE LA POSTURA INSTITUCIONAL ANTE EVENTOS QUE HAN AFECTADO LA CONTINUIDAD DE LA PRESTACIÓN DE SERVICIOS

Este Órgano Fiscalizador evidenció oportunidades de mejora en la dirección y coordinación de acciones dirigidas en forma integral desde el ámbito estratégico como respuesta a eventos de impacto a la continuidad de los servicios proporcionados por la CCSS. Específicamente, en lo que corresponde a una estrategia integrada para fortalecer la postura institucional frente a situaciones de emergencia, desastre, crisis, y otros eventos similares.

Todo lo anterior, en aras de orientar al conjunto de involucrados en fortalecer la capacidad de la institución para anticipar, prepararse y responder de manera efectiva a eventos de riesgo en la continuidad de sus operaciones a nivel de negocio, considerando lecciones aprendidas ante situaciones como la experimentada durante el ciberataque sufrido en mayo del 2022.

Pese a identificarse documentos con el registro de lecciones aprendidas, estrategias implementadas y propuestas de mejora, como el oficio GA-1105-2022 del 27 de setiembre de 2022, no se ha elaborado un documento que consolide toda la información de la CCSS y a partir de ello se haya dado origen a un plan de fortalecimiento integral. Además, se notaron labores gestadas por la Administración en torno al fortalecimiento de la postura institucional, pero se centran en recordatorios y actualizaciones de los planes de continuidad en TIC; aunque estas acciones son pertinentes, no abordan completamente los aspectos necesarios para robustecer la preparación en eventos de emergencia, dejando sin atender importantes asuntos relacionados con el proceso de negocio.

En ese sentido, el plan de fortalecimiento esperable de este tipo de situaciones debería estar orientado a proteger a la CCSS, sus funcionarios, usuarios y la ciudadanía en general, mediante la implementación de mejoras en materia de resiliencia operativa, identificación de servicios críticos, gestión de riesgos, recuperación rápida, comunicación efectiva, entre otros aspectos no menos importantes.

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el inciso 4.1 "Actividades de control" indica:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el

fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad. El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la institución. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante."

Además, esas mismas normas, en el inciso 6.4 "Acciones para el fortalecimiento del SCI" indica:

"Cuando el funcionario competente detecte alguna deficiencia o desviación en la gestión o en el control interno, o sea informado de ella, debe emprender oportunamente las acciones preventivas o correctivas pertinentes para fortalecer el SCI, de conformidad con los objetivos y recursos institucionales. Así también, debe verificar de manera sistemática los avances y logros en la implementación de las acciones adoptadas como producto del seguimiento del SCI."

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado I. Gobernanza, señala:

"La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales".

El perfil funcional del Centro de Atención de Emergencias y Desastres (CAED) publicado en el 2016, refiere en cuanto funciones sustantivas de la unidad , lo siguiente:

"- Realizar acciones orientadas a prevenir en la Institución la ocurrencia de emergencias y desastres, con el objeto de proteger la vida de las personas y los diferentes recursos."

El Dr. Mario Vílchez Madrigal, Director a.i del Centro de Atención de Emergencias y Desastres -CAED, mencionó sobre la generación de insumos relacionados con lecciones aprendidas tras el ciberataque:

"Los espacios para dialogar y generar los insumos relacionados con las lecciones aprendidas tras el ciberataque siempre han estado ahí. De hecho, con la DTIC tenemos una relación de colaboración que data, al menos, de la atención de la Tormenta Tropical Nate en el 2017, y que yo puedo catalogar como muy cercana. Como le mencioné en la conversación que tuvimos la semana pasada, por las características de este evento en particular, y de la forma en que se direccionó la atención de esta emergencia desde la GG, la DTIC y los CGI´s fue poco lo que pudimos aportar. Hasta donde yo tengo entendido, si se han realizado varios esfuerzos para recopilar esas lecciones aprendidas durante el ciberataque. Otros factores que pueden haber sido limitantes son los cambios en la estructura organizacional, por ejemplo, la Gerencia General, las diferentes adscripciones que ha tenido la DTIC, y los cambios de dirección de la DTIC (4 directores diferentes desde el ciberataque a la fecha). Finalmente, muchos de los productos que nosotros generamos no están específicamente diseñados para el negocio DTIC, por lo que se podría percibir que lo que nosotros podemos aportar no necesariamente es lo que la DTIC está requiriendo."

La ausencia de un fortalecimiento efectivo en la postura institucional frente a eventos que puedan tener un impacto en la continuidad de la prestación de servicios revela vulnerabilidades significativas en la operación de la institución. Este déficit afecta negativamente la capacidad de la organización para abordar los desafíos, implementar mejoras continuas y prepararse adecuadamente ante sucesos similares.

En consecuencia, disminuye su capacidad para fortalecer la resiliencia organizacional a través de un direccionamiento y abordaje integral del tema.

5. EVALUACIÓN DE RIESGOS RELACIONADOS CON AMENAZAS DE CIBERSEGURIDAD

Se constató que, durante el año 2022, según revisión efectuada a la información registrada a nivel general de la CCSS en las herramientas de "Valoración de Riesgos"[9], únicamente 5 riesgos (equivalente al 0,5% del total de riesgos identificados en la categorización TIC) fueron vinculados con causas donde se mencionaba la probabilidad de ocurrencia de un ataque informático.

En este contexto, resalta la falta de un enfoque proactivo en la identificación y gestión de riesgos en seguridad informática por parte de la Administración Activa y consecuentemente detectar cualquier desvío que le impida a la CCSS la consecución de sus objetivos.

Ahora bien, al examinar la identificación y evaluación de riesgos llevada a cabo para el año 2023, los funcionarios responsables, tras haber sido afectados por cibercrimen y enfrentar la incapacidad de acceder a los servicios TIC de manera habitual, especifican un total aproximado de 169 causas (13% del total de causas y/o riesgos identificados) interrelacionadas con posibles ciberataques, como se detalla en la tabla siguiente:

Tabla No. 3
Total de riesgos TIC vinculados a causas motivados por Ciberataques, 2023

Región	Cantidad de riesgos
Brunca	25
Central Norte	21
Central Sucursales	1
Central Sur	22
Chorotega	5
Chorotega sucursales	1
Hospitales Especializados	15
Hospitales Nacionales	14
Huetar Atlántica	4
Huetar Norte	4
Huetar Norte Sucursales	3
Nivel Central	44
Pacífico Central	10

Si bien es evidente que ha habido un aumento significativo en la cantidad de riesgos identificados entre los periodos (en 2022 se registraron un total de 886 riesgos y en el 2023 se contabilizan 1341), la conciencia y el enfoque en la valoración no deben limitarse a la ocurrencia de eventos. Por el contrario, se aboga por una labor preventiva y anticipada, permitiendo gestionar de manera oportuna, razonable y efectiva la exposición al riesgo.

La Ley General de Control Interno, Artículo 14 Valoración del riesgo, señala:

> *"En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:*

[9] Herramientas de valoración de Riesgos 2022 oficializada por el Área Gestión de Control Interno en la cual los titulares subordinados de la CCSS, identifica y valora los riesgos operativos de los servicios institucionales.

a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.
b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.
c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.
d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar."

Las Normas de Control Interno para el Sector Público en el Capítulo III: Normas sobre valoración del riesgo, indican:

"3.1 Valoración del riesgo. El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure.

3.2 Sistema específico de valoración del riesgo institucional (SEVRI). El jerarca y los titulares subordinados, según sus competencias, deben establecer y poner en funcionamiento un sistema específico de valoración del riesgo institucional (SEVRI). El SEVRI debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable. Asimismo, debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento.

3.3 Vinculación con la Planificación institucional. La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y, en consecuencia, de los riesgos correspondientes."

Desde la perspectiva de esta Auditoría, la omisión en la identificación de riesgos potenciales asociados a las Tecnologías de Información y Comunicaciones podría ser causada por varios factores. Entre ellos se encuentra la falta de conciencia sobre la importancia de la gestión de riesgos a nivel local, debilidades en la cultura organizacional en la priorización de la seguridad informática como un tema crítico institucional y mantener un enfoque reactivo en lugar de proactivo. Además, de la insuficiencia de capacitación, habilidades y conocimientos necesarios para reconocer y abordar riesgos de manera efectiva.

Si esta situación persiste, la CCSS enfrentaría consecuencias significativas al aumentar la probabilidad de materialización de amenazas no identificadas, lo que conllevaría a brechas de seguridad, pérdida de datos, interrupciones operativas y deterioro de la reputación.

Por otra parte, la debilidad en la cultura de valoración de riesgos puede conducir a la implementación ineficaz de controles de seguridad, disminuyendo la capacidad de anticipar y responder a desafíos, generando consecuencias financieras, legales y operativas adversas para la institución.

6. SOBRE LA SUBÁREA DE CONTINUIDAD DE LA GESTIÓN

Esta Auditoría Interna constató las siguientes debilidades en la Subárea de Continuidad de la Gestión, adscrita a la DTIC:

- **Sobre las condiciones de la plaza de jefatura**

  Desde el año 2020, la plaza de Jefe de la Subárea de Continuidad de la Gestión (Jefe en TIC 1) ha permanecido inactiva. Inicialmente, fue justificada por la necesidad de reactivarla, pero la Gerencia General posteriormente decidió no respaldar su utilización debido a la incertidumbre asociada a los cambios organizacionales en curso y considerando que únicamente tendría un subalterno a cargo.

- **Disposición de Personal técnico en la Subárea de Continuidad de la Gestión**

  La Subárea de Continuidad de la Gestión no dispone de personal técnico debido a que la única plaza asignada formalmente fue trasladada desde el 31 de mayo de 2022 (más de 17 meses a la fecha) a la Subárea de Seguridad TI, en apoyo a las necesidades prioritarias derivadas del ciberataque.

- **Falta de evaluaciones a los planes de continuidad:**

  No se han efectuado evaluaciones a los planes de continuidad desarrollados e implementados, desde el 2021.

En otras palabras, las circunstancias en las que se ha mantenido la Subárea de Continuidad de la Gestión no están respondiendo de manera adecuada a las necesidades cruciales de la institución para fortalecer su resiliencia y preparación ante la respuesta, contingencia y continuidad que debe existir desde el ámbito que corresponde a las Tecnologías de Información y Comunicaciones.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado XI. Seguridad y Ciberseguridad, señala:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados."*

Además, en ese mismo marco normativo, en el inciso XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, indica:

> *"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."

A ese respecto, el Ing. Daniel Berrocal Zúñiga, jefe del Área de Seguridad y Calidad Informática, mencionó:

"Mediante Resolución Administrativa No. GG-DTIC-7740-2023 firmada en fecha 22 de noviembre de 2023, se realiza el traslado del Ing. Jason Rojas Solano con la plaza No. 34264 en el perfil de analista en sistemas 4 TIC al Área de Seguridad y Calidad de la DTIC, por lo cual mediante el oficio No. GG-DTIC-7868-2023 de fecha 23 de noviembre de 2023, se le solicita realizar un diagnóstico y plan de trabajo de la Subárea de Continuidad de la Gestión en TIC, para abordar las funciones sustantivas de la Subárea que se han dejado de desarrollar por la falta de recurso humano. Se le solicita presentar este diagnóstico para valoración de la jefatura del Área de Seguridad y Calidad Informática a más tardar el 16 de febrero de 2024, este diagnóstico debe ir acorde a las funciones sustantivas de la Subárea de Continuidad de la Gestión en TIC de acuerdo con el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones (…)

Como se puede evidencia en lo supra señalado esta Subárea no ha contado con la cantidad de recurso humano suficiente para llevar adelante el desarrollo de sus funciones sustantivas señalas en el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, así como también el apoyo que se brindó para el levantamiento de los servicios después del evento de seguridad del pasado 31 mayo de 2022, sin embargo, con el traslado del recurso humano señalado el área estará asumiendo las funciones de la Subárea de Continuidad de la Gestión en TIC para que se logre de manera correcta el cumplimiento de las funciones establecidas según el Manual de Organización."

La persistencia de la actual situación en la Subárea de Continuidad de la Gestión en TI, adicional al debilitamiento del sistema de control interno y la desatención de normativa aplicable, aumenta la posibilidad de materialización de riesgos orientados a la preparación institucional para garantizar la continuidad de tecnologías que soportan la operativa de sistemas informáticos y servicios digitales y por ende, la prestación de servicios médicos y de pensiones a la población costarricense. Lo anterior ante la falta de actores y/o unidades institucionales que lleven la responsabilidad de coordinar acciones en ese sentido, así como el restablecimiento de servicios afectados en el menos tiempo posible.

7. NORMATIVA QUE SUSTENTA LA EJECUCIÓN DE PLANES DE ACCIÓN EN MATERIA DE LA RESPUESTA, CONTINGENCIA Y CONTINUIDAD A NIVEL DE NEGOCIO Y TECNOLÓGICO

Se identificaron oportunidades de mejora en la formulación y actualización del marco normativo, así como otros documentos conexos que respaldan la implementación de planes destinados a regular la continuidad y contingencia de los servicios proporcionados por la Caja en los ámbitos de salud, pensiones y recaudación patronal.

A continuación, se presentan las principales debilidades identificadas en los documentos regulatorios, destacándose el período de hasta 17 años transcurridos sin que se haya llevado a cabo la actualización tanto del marco normativo asociado al contexto del negocio como del correspondiente a Tecnologías de la Información y Comunicaciones.

Tabla No. 4
Actualización del marco normativo y documentación de apoyo a fines con los planes de respuesta, contingencia y continuidad a nivel de negocio y tecnológico

Marco regulatorio	Fecha de emisión y/o última actualización	Observaciones
Política de Hospital Seguro de la CCSS	6 de julio del 2006	Han pasado 17 años desde la emisión de este manual, y hasta la fecha actual, no se ha realizado ninguna revisión ni actualización de este. Sin embargo, el CAED se encuentra en la ejecución de la recomendación 1 del informe AAS-076-2022 tomando la decisión de renovar la política para el 1er semestre del 2024.
Políticas Institucionales de Seguridad Informática TIC-Seguridad-001, Versión 1.0	Octubre 2007	Han pasado 16 años desde la emisión de este manual, y hasta la fecha actual, no se ha realizado ninguna revisión ni actualización de este.
Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002, Versión 1.0	Abril 2008	Han pasado 15 años desde la emisión de este manual, y hasta la fecha actual, no se ha realizado ninguna revisión ni actualización de este.
Política para la Organización de la respuesta a Emergencias y Desastres en la Caja Costarricense de Seguro Social.	25 de marzo del 2010	Han pasado 13 años desde la emisión de este manual, y hasta la fecha actual, no se ha realizado ninguna revisión ni actualización de este.
Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, ASCI-UCG-0RG-002, Versión 2.4	Mayo 2013	Han pasado 10 años desde la emisión de este manual, y hasta la fecha actual, no se ha realizado ninguna revisión ni actualización de este.

Fuente: Elaboración propia a partir de la información remitida por la administración activa e información extraída de la intranet institucional.

En ese sentido se observa como el marco normativo dentro de la gestión operativa y estratégica carece de actualización y una orientación multiamenaza que permita gestionar de manera proactiva e integral las acciones institucionales ejecutadas en respuesta a emergencias y desastres en forma ágil y efectiva.

La Ley 8292: Ley General de Control Interno, artículo 15. Actividades de control, indican lo siguiente:

"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:
a) ***Documentar, mantener actualizados y divulgar internamente****, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*
b) ***Documentar, mantener actualizados y divulgar internamente*** *tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*

i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.
ii. La protección y conservación de todos los activos institucionales.

iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.
iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.
v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación" ***El resaltado no pertenece al original.***

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el inciso 1.4 "Responsabilidad del jerarca y los titulares subordinados sobre el SCI" indica:

"La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.

En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes: (…)

c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y ***actualizados****, y sean divulgados y puestos a disposición para su consulta."* ***El resaltado no pertenece al original.***

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021, en el apartado "Procesos del marco de Gestión de TI", establece en relación con la "Calidad de los procesos tecnológicos", lo siguiente:

"La institución debe implementar prácticas que permitan controlar los procesos organizacionales, posibilitando la mejora continua de productos y servicios, buscando asegurar la satisfacción de las necesidades institucionales, manteniendo estándares de documentación de los lineamientos requeridos, esquemas para la medición del desempeño y control sobre la vigencia de las prácticas aplicables a los procesos.

Igualmente, debe generar servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo de los procesos que habilitan la gestión de las tecnologías de información."

El perfil funcional del Centro de Atención de Emergencias y Desastres (CAED) publicado en el 2016, refiere en cuanto funciones sustantivas de la unidad, lo siguiente:

"-Formular, actualizar, controlar y evaluar las políticas, las estrategias y los lineamientos emitidos en materia de emergencias o desastres, con la finalidad de prevenir y disminuir las consecuencias de un evento y orientar la toma de decisiones.

-Administrar, actualizar, articular, controlar y evaluar, en coordinación con las diversas instancias de la Institución, la Política de Hospital Seguro, el Plan Institucional de Emergencias, la Política para la organización y respuesta de emergencias y desastres, entre otras de esta naturaleza, a efecto de disponer de instrumentos actualizados que orienten las acciones ante la ocurrencia de un evento y proponer a las autoridades superiores los ajustes a la normativa que se consideren pertinentes y facilitar la continuidad de los servicios."

- Promover que las diversas instancias de la Institución realicen los diagnósticos y las evaluaciones estructurales, no estructurales y funcionales, con el objeto de identificar los riesgos, amenazas y vulnerabilidades inherentes a los procesos y actividades críticas, determinar la capacidad de respuesta de los niveles central, regional y local, ante la ocurrencia de eventuales emergencias y desastres y facilitar el diseño de los planes de acción y la continuidad en la prestación de servicios.

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Seguridad y Calidad Informática (ASCI), establece:

"Formular, actualizar y evaluar la regulación, la normativa técnica, los protocolos y los estándares en su ámbito de competencia, con base en la normativa aprobada por el Consejo de Presidencia y de Gerentes, la tecnología en uso y los procesos de investigación, con el propósito de lograr uniformidad en los sistemas y maximización de los recursos institucionales.

(…) - Actualizar la documentación técnica en su ámbito de competencia, con base en los requerimientos de la organización, la normativa aprobada en el Consejo de Presidencia y de Gerentes, las políticas y estrategias vigentes, con el objeto de lograr la operación efectiva de los sistemas de información institucionales."

El Dr. Mario Vílchez Madrigal, quien ocupa el cargo de Director en funciones en el Centro de Atención de Emergencias y Desastres (CAED), indicó:

"La Política de Hospital Seguro ha sido objeto de varios informes de Auditoría, y como resultado de la última, se le solicitó a la Gerencia General realizar el análisis de exactamente lo que usted está consultando. La Gerencia General trasladó la atención de ese análisis al CAED. Se estableció un grupo de trabajo Intergerencial, se determinó que dicha Política debía ser actualizada, y dicha conclusión fue trasladada a la Gerencia General. Actualmente se está trabajando en la actualización de dicha Política"

Por otra parte, el Ing. Daniel Berrocal Zúñiga, jefe del Área de Seguridad y Calidad Informática, mencionó:

"Esta Área reconoce la importancia de revisar y actualizar toda la documentación y normativa TIC, con respecto a las funciones sustantivas de la Subárea de Continuidad de la Gestión en TIC, es por esta razón que estará realizando su mejor esfuerzo para realizar una actualización y cumplimiento de esta función"

En este contexto, la ausencia de normativa o la falta de su actualización potencialmente afecta de manera adversa la eficiencia operativa, el cumplimiento regulatorio, la toma de decisiones y la capacidad de adaptación de la CCSS. Es decir, de mantenerse este escenario se incrementa los riesgos y podría obstaculizarse la capacidad de la institución para alcanzar sus objetivos de manera efectiva.

CONCLUSIONES

Esta Auditoría a través del presente estudio referente al restablecimiento de sistemas de información y servicios tecnológicos posterior al ciberataque del 2022, evidenció oportunidades de mejora en la gestión de emergencias, destacando la importancia de que la institución sea proactiva ante riesgos, independientemente de su origen, y utilizar la experiencia de la intrusión digital perpetrada en el 2022 como un impulso capaz de fortalecer la continuidad del negocio.

En primera instancia, se identificó que el Programa de Gobernanza y Gestión de las TIC, específicamente en la iniciativa "Habilitar la gestión de la continuidad del negocio", no ha avanzado desde 2018. Esta situación representa un desafío significativo, ya que limita la obtención inmediata de beneficios relacionados con la garantía razonable de establecer actividades competentes para impulsar la continuidad del negocio, lo cual de darse de manera adecuada podría mitigar gran parte de los hallazgos identificados en la presente evaluación.

Además, se identificó la falta de planes específicos para la gestión de emergencias a nivel institucional con un enfoque integral que asuma la responsabilidad de asegurar la respuesta, contingencia y continuidad, independientemente de si interactúan o no las Tecnologías de la Información (TI). Es decir, esto implica la necesidad de contar con planes de respuesta, contingencia y continuidad diseñados para mantener las operaciones críticas, incluso en situaciones donde los sistemas tecnológicos puedan verse o no comprometidos.

No obstante, destaca la necesidad de realizar evaluaciones y planes de mejora integrales y estandarizados, especialmente después del ciberataque, para detallar las áreas afectadas en términos de productividad, reputación y aspectos normativos, entre otros. Lo cual, se origina ante la falta de una metodología que respalde el despliegue de manera oportuna información consolidada para facilitar la toma de decisiones a nivel estratégico y táctico.

En este sentido, es criterio de esta Auditoria que es imperativo desarrollar estrategias de mejora en la comunicación con el fin de notificar eficientemente a las partes pertinentes. Asimismo, establecer un monitoreo continuo para identificar debilidades u oportunidades y a partir de ello, extraer lecciones aprendidas de manera efectiva.

Por otra parte, se observaron limitaciones sustanciales en la Subárea de la Continuidad de la Gestión, las cuales se atribuyen a la disponibilidad de personal para apoyar las labores encomendadas a la unidad. Esta asignación ha tenido como consecuencia la paralización de funciones fundamentales de la Subárea por más de 17 meses, como las evaluaciones a los planes de continuidad en el ámbito de las Tecnologías de la Información a nivel institucional.

Finalmente, en el ámbito normativo en materia de continuidad del negocio se destaca el riesgo asociado a la desactualización prolongada del conjunto de documentos que lo conforman, lo que representa un desafío para garantizar un respaldo efectivo de los procesos institucionales que pretende apoyar.

En virtud de lo anterior y en conformidad con el marco regulatorio aplicable, esta Auditoría propone una serie de recomendaciones con el fin de que sean consideradas por la administración para coadyuvar en la mitigación de los riesgos identificados en el presente estudio.

RECOMENDACIONES

A LA MÁSTER MARTA EUGENIA ESQUIVEL RODRÍGUEZ, EN SU CALIDAD DE MÁXIMA AUTORIDAD DEL CONSEJO TECNOLÓGICO DE LA CCSS O A QUIEN EN SU LUGAR OCUPE SU CARGO.

1. De conformidad con lo señalado en los hallazgos 1, 2 y 5 de este estudio, según el marco regulatorio aplicable y posibilidades institucionales, siendo que el Consejo Tecnológico tiene a su cargo la coordinación de temas estratégicos relacionados con el "Modelo Meta de Gobernanza y Gestión de las TIC" y en virtud de que la iniciativa "Habilitar la gestión de la continuidad del negocio" aún no ha iniciado su diseño e implementación; establecer el mecanismo de control y seguimiento adecuado que permita garantizar razonablemente el inicio y/o avance de esa iniciativa.

   Para tales efectos, es esencial garantizar la formalización de al menos las siguientes actividades:

   - Definición del conjunto de responsables a cargo del diseño e implementación de la iniciativa (según corresponda, con representación de los niveles organizacionales que propone la iniciativa y ese Órgano Colegiado considere).
   - Establecer una estrategia de sensibilización a la alta administración de la importancia de la continuidad de negocio y sus responsabilidades asociadas.

- Definición del conjunto de responsables a cargo de la iniciativa (en el ámbito de negocio y tecnológico) con representación de todos los niveles organizacionales a los que corresponde la responsabilidad de continuidad de los servicios a nivel institucional.
- Consolidar los proyectos y esfuerzos que la institución está llevando a cabo en relación con temas vinculados a la administración del riesgo, tanto en el ámbito preventivo como correctivo, que aún no han sido interrelacionados con la iniciativa de marras.
- Establecimiento de un cronograma que apoye el desarrollo de tareas y actividades alineadas a las necesidades de la CCSS para la consecución exitosa de la iniciativa.
- Priorizar (según corresponda) el desarrollo de la iniciativa, considerando las situaciones que se le han presentado en la CCSS desde la pandemia por Covid-19 hasta el Ciberataque perpetrado en mayo del 2022, en ambos casos sin existir un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), con enfoque multiamenaza.
- Desarrollar una campaña de concientización sobre la importancia de brindar un enfoque integral en la gestión de riesgos (Identificación, análisis y evaluación de riesgos; planificación e implementación de respuestas; monitoreo y control).

Bajo la premisa de ejercer control y seguimiento, se sugiere solicitar de manera periódica un informe (definir la frecuencia) que describa el avance en el desarrollo de la implementación de la iniciativa, incluyendo logros alcanzados, resultados obtenidos y desviaciones, hasta llegar a determinar el cumplimiento del objetivo planteado para habilitar la gestión de la continuidad del negocio.

Para acreditar el cumplimiento de la presente recomendación, deberá enviar a este Órgano de Fiscalización **en un plazo de 10 meses** a partir de la recepción del informe, la documentación formalizada de las actividades supracitadas en la que se defina el desarrollo de la iniciativa, “Habilitar la gestión de la continuidad del negocio”.

AL MÁSTER ROBERT PICADO MORA, SUBGERENTE DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES, O A QUIEN EN SU LUGAR OCUPE EL CARGO

2. De conformidad con el hallazgo 6, establecer los mecanismos de control y supervisión necesarios para asegurar la correcta ejecución de las actividades coordinadas por el Área de Seguridad y Calidad Informática, referentes a la obtención del diagnóstico situacional de la Subárea de Continuidad de la Gestión y su eventual plan de trabajo correspondiente a remediar las condiciones actuales de la instancia técnica supracitada. Lo anterior en coordinación con las instancias institucionales pertinentes.

   Con base en esta información, esa Dirección deberá revisar y avalar formalmente los resultados obtenidos y plan de acción propuesto para asegurar el cumplimiento eficaz de las responsabilidades asignadas a la Subárea de Continuidad de la Gestión en TIC.

   Para acreditar el cumplimiento de la presente oportunidad de mejora, debe remitirse a esta Auditoría en un **plazo de 6 meses** a partir de la fecha de recepción del estudio, el respaldo documental sobre los mecanismos de control y supervisión que se aplicarán por parte de la Dirección de Tecnologías de Información y Comunicaciones y el aval otorgado al plan de trabajo remitido por el Área de Seguridad y Calidad Informática para remediar las condiciones actuales de la Subárea de Continuidad de la Gestión.

3. De conformidad con las iniciativas del programa de gobernanza y gestión TI que refieren al desarrollo y actualización de lineamientos y normativa, instruir al conjunto de responsables para formalizar un plan de trabajo con plazos, responsables y actividades que apoye la premisa de revisar, modificar, ajustar y/o actualizar de forma integral el marco normativo citado en el hallazgo 7 relacionado a la seguridad TIC y planes de continuidad de la gestión en TI.

Para acreditar el cumplimiento de la presente oportunidad de mejora, debe remitirse a esta Auditoría en un **plazo de 9 meses** a partir de la fecha de recepción del estudio, el plan de trabajo supracitado que respalde la revisión y actualización del marco regulatorio.

A DOCTOR MARIO VÍLCHEZ MADRIGAL, EN SU CALIDAD DE DIRECTOR A CARGO DEL CENTRO DE ATENCIÓN DE EMERGENCIAS Y DESASTRES O QUIEN EN SU LUGAR OCUPE SU CARGO.

4. En concordancia con los hallazgos 3 y 4, efectuar un análisis sobre la necesidad de implementar mecanismos documentales estandarizados que respalden el marco normativo actual del CAED en cuanto al diseño e implementación de plantillas que apoyen de forma integral la recopilación, presentación, consolidación y validación de información proveniente de las gerencias institucionales para evaluar la situación y tomar de decisiones por parte de la Junta Directiva, la Presidencia Ejecutiva, el Consejo de Presidencia, el Consejo Tecnológico, Auditoría Interna, entre otros grupos de interesados ante situaciones que puedan afectar la prestación de servicios de salud, pensiones y recaudación patronal.

   Para tales efectos, es esencial garantizar la formalización en un plan de acción con el detalle de las siguientes actividades:

   - Desarrollo de plantillas y/o guías, referentes a la recopilación, presentación, actualización de datos, seguimiento a recomendaciones o planes de fortalecimiento, entre otros asuntos.
   - Identificación de indicadores clave y métricas relevantes para la toma de decisiones, tales como: impacto, tiempos transcurridos, personal involucrado, equipos y recursos desplegados, afectación en la productividad de los funcionarios, evaluación de daños, afectación en las comunicaciones, lecciones aprendidas, costos asociados, cobertura tecnológica, utilización de pólizas, entre otras métricas.
   - Socialización y/o recordatorios de la normativa vigente, así como de la notificación correspondiente a las mejoras y/o modificaciones aplicadas al marco regulatorio.

   Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un **plazo de 8 meses**, a partir de la recepción del presente informe, la documentación que respalde en la valoración efectuada y los acuerdos para formalizar el plan de acción orientado a mejorar al proceso que refiere al análisis integral, consolidar lecciones aprendidas y/o generar planes de fortalecimiento en apoyo a la toma de decisiones, contribuyendo así con la resiliencia institucional y mejora continua.

5. De conformidad con el hallazgo 7, establecer un plan de trabajo con el detalle de plazos, responsables y actividades que apoye la premisa de revisar, modificar, ajustar y/o actualizar el marco normativo emitido por el Centro de Atención de Emergencias y Desastres (según corresponda).

   Para acreditar el cumplimiento de la presente oportunidad de mejora, debe remitirse a esta Auditoría en un **plazo de 7 meses** a partir de la fecha de recepción del estudio, el plan de trabajo supracitado que respalde la revisión y actualización del marco regulatorio.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 62 del Reglamento de Organización y Funcionamiento de la Auditoría Interna de la Caja Costarricense de Seguro Social, los resultados del presente informe fueron comentados el 13 de diciembre de 2023 con la Licda. Angeline Badilla Berrocal, Asesora Presidencia Ejecutiva; Máster Christian Chacón Rodríguez, Subdirector de la DTIC; Dr, Mario Vílchez Madrigal, Director del CAED.

Respecto a los hallazgos presentados no se emitieron observaciones o comentarios.

Sobre las recomendaciones se hicieron las siguientes observaciones:

Recomendación 1: La Licda. Badilla, solicita criterio de la DTIC para indicar si se debe ampliar el plazo de la recomendación.

El Máster Chacón, indica que el plazo propuesto por la Auditoría de 10 meses es razonable.

Recomendación 2: No hay observaciones.

Recomendación 3: El Máster Chacón, solicita se amplie el plazo para acreditar el cumplimiento de la presente recomendación, a 9 meses.

El Ing. Herrera, accede a la modificación del plazo de atención de la recomendación a 9 meses.

Recomendación 4: No hay observaciones.

Recomendación 5: El Dr. Vílchez, solicita se amplie el plazo para acreditar el cumplimiento de la presente recomendación, a 7 meses.

El Ing. Herrera, accede a la modificación del plazo de atención de la recomendación a 7 meses.

Las observaciones emitidas por la administración fueron valoradas e incorporadas por esta Auditoría en el presente informe. Respecto de las recomendaciones en las que no se efectuaron observaciones, se aceptaron los términos establecidos en forma, fondo, plazo y entregables para su atención.

OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Firmado digitalmente por OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Fecha: 2023.12.14 16:08:01 -06'00'

Lic. Oscar Mena Granados
Asistente de Auditoría

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2023.12.14 16:42:45 -06'00'

Lic. Rafael Ángel Herrera Mora, jefe
Área Tecnologías de Información y Comunicaciones

OSC/RJS/RAHM/OMG/jrc