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

AS-AATIC-116-2022
07 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA-2901

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA-1103

Licenciado
Luis Fernando Campos, gerente
GERENCIA ADMINISTRATIVA-1104

Doctor
Esteban Vega de la O, gerente
GERENCIA LOGÍSTICA-1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

Máster
Idannia Mata Serrano, subgerente a.i,

Máster
Vanessa Carvajal Carmona, jefe a.i.
Subárea Seguridad de Tecnologías de Información
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150.

Estimados señores(as):

ASUNTO: Oficio de Asesoría referente a los Planes de Continuidad de TIC.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre la implementación, ejecución y utilización de los Planes de Continuidad de la Gestión en TIC en las unidades, como respuesta administración activa.

En ese sentido, este órgano de fiscalización efectuó una revisión de los productos de auditoría emitidos a nivel institucional donde se mencionaron aspectos de mejora sobre la existencia, aprobación, ejecución y utilización de los Planes de Continuidad de la Gestión en TIC, además, se consultó a 58 unidades institucionales (hospitales, áreas de salud y sucursales), sobre este mismo tema. Lo anterior, con el propósito de efectuar un diagnóstico situacional de las medidas adoptadas para garantizar la continuidad en la prestación de los servicios médico – administrativos en la Caja Costarricense de Seguro Social.

Al respecto, los resultados obtenidos son los siguientes:

I. ANTECEDENTES

El Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones (mayo 2013), en su apartado “Introducción”, se indica:

> *“La criticidad de la información dentro de la organización y la complejidad de los sistemas de información hacen que las organizaciones sean más sensibles ante las amenazas de la integridad de la información. Los incidentes de perdida de información que con cierta frecuencia se presentan y son dados a conocer por los medios de comunicación, provocan alarma en las Organizaciones ya que afectan a la totalidad de las actividades de estas. Sin embargo, incidentes menos relevantes como el fallo de una línea de comunicación puede tener un efecto devastador en los procesos de la organización.*
>
> *En la actualidad la regulación de la mayoría de los sectores no suele hacer una referencia específica a la continuidad de negocio. En general, los administradores suelen poner énfasis en la integridad y disponibilidad de la información más que en la disponibilidad de los sistemas como base a la continuidad del negocio de la empresa.*
>
> *Ante esta realidad la Dirección de Tecnologías de Información y Comunicaciones ha visto la necesidad de buscar soluciones que obedezcan a estrategias que aseguren la seguridad y continuidad de sus procesos operativos sustantivos (…)*
>
> *El enfoque principal de un Plan de Continuidad en TIC considera recuperar las operaciones de los procesos sustantivos de una organización, dentro de un espacio de tiempo determinado, buscando equilibrar el costo y viabilidad de éste.*
>
> *Cabe mencionar que la generación de un Plan de Continuidad en TIC tiene una relación muy estrecha con la alta gerencia de la organización, ya que el éxito de este tipo de prácticas organizacionales depende en gran medida, del grado de involucramiento de estos actores”.*

A nivel externo de la institución1, se establece dentro de los conceptos de Plan de Continuidad en TIC, lo siguiente:

[1] Información extraída de páginas web de empresariales SOTHIS, SafetyCulture, WTW y APSER Cloud Service.

"(…) El Plan de Continuidad se convierte en un mecanismo sustantivo para mantener en operación el conjunto de procesos, procedimientos, asegurar los recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro; un Plan de Continuidad, es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las Comunicaciones que tiene como fin, garantizar la continuidad de los servicios de TI (…)".

Asimismo, se indica:

"(…) el Plan de Continuidad de las Tecnologías de la Información y las Comunicaciones el cual consistiría en una estrategia planificada, constituida por un conjunto de recursos y procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan los procesos de negocio considerados como críticos en la Institución".

Además, se mencionan una serie de beneficios que trae a las instituciones u organizaciones la elaboración de Planes de Continuidad en TIC, donde se detallan, entre otros:

- *"Protección de la viabilidad de la gestión al enfrentar una interrupción mayor, mediante una estrategia de continuidad.*
- *Aprovechamiento de la infraestructura actual para ese objetivo.*
- *Aprovechamiento de la documentación actual (procesos y procedimientos).*
- *Equilibrio entre las variables: costo, beneficio y riesgo.*
- *Definición de una estructura organizacional para el Plan de Continuidad de la Gestión en TIC.*
- *Diseño de medidas para reducción de riesgos identificados.*
- *Definir una estrategia global de continuidad de negocio, basada en la recuperación de la operación y servicios sustantivos de cualquier organización.*
- *Selección de componentes para cumplir con la estrategia de continuidad.*
- *Creación de una cultura de continuidad de negocio.*
- *Contar con planes de continuidad de negocio, los cuales podrán ayudar a la organización a operar sus procesos más críticos de negocio durante un periodo contingente.*
- *Contar con análisis de riesgo e impacto de los componentes (activos) que soportan al proceso.*
- *Identificar los puntos más críticos y vulnerables de los procesos de negocio de la organización.*
- *Identificar áreas de oportunidad dentro de la organización, como resultado de los análisis y alternativas de operación durante un periodo contingente.*
- *Cálculos sobre el costo aproximado de pérdida, al no poder ejecutar un proceso crítico (…)".*

En relación con lo anterior, es importante mencionar que según lo detallado el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, le corresponde a la Subárea de Continuidad de la Gestión, brindar el seguimiento, gestión y control de la Continuidad de los servicios TIC en la Institución.

Al respecto, a los diferentes actores involucrados en la Dirección de Tecnologías de Información y Comunicaciones, Área de Seguridad y Calidad Informática, Subárea de Continuidad de la Gestión, Centros de Gestión Informática Gerencial, Centros de Gestión Informática Regional y Local, entre otros, les han sido asignadas, mediante los manuales de organización respectivos, las funciones sustantivas asociadas al tema de marras.

Por otra parte, como ya es conocido, entidades públicas tales como: Ministerio de Hacienda, Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT) y la Caja Costarricense de Seguro Social, han sido blanco de múltiples ataques tipo ransomware, que impide a los usuarios e instituciones acceder a sus sistemas o archivos exigiendo el pago de un rescate para poder disponer nuevamente de ellos.

El 31 de mayo de 2022, se registró en horas de la madrugada un ciberataque contra los servidores de la C.C.S.S., el cual obligó a realizar una desactivación controlada de los servicios TI institucionales, de acuerdo con los informes presentados por la Dirección de Tecnologías de Información y Comunicaciones al Centro Coordinador de Emergencias Institucional (CCEI); además, se solicitó mantener apagados los equipos de cómputo que estuviesen conectados a la red institucional, a fin de que los profesionales en Tecnologías de la Información y Comunicación efectuaran un diagnóstico y determinar el nivel de afectación.

II. RESULTADOS OBTENIDOS

2.1 Productos emitidos por la Auditoría:

En relación a este tema, la Auditoría Interna ha señalado a la administración activa la importancia de examinar el alcance, desarrollo, aprobación, implementación y seguimiento de los Plan de Continuidad de la Gestión en Tecnologías de Información, así como la relevancia de garantizar la contingencia de los servicios tecnológicos, realizando en diversas ocasiones recomendaciones y asesorías con el fin de fortalecer las medidas para atender las oportunidades de mejora, establecidas en diversas unidades y procesos institucionales. En **el anexo 1** se indican algunos de los productos en los que se abordaron, de manera total o parcial, la temática anteriormente mencionada.

Asimismo, a nivel operativo o local, la auditoría interna ha emitido algunos productos que se indican en el anexo 2, en los que se menciona los Planes de Continuidad de TIC implementados por los Centros de Gestión Informática de las unidades evaluadas.

2.2 Sobre el rol y responsabilidades de la Subárea de Continuidad de la Gestión

En relación con lo anterior, es importante mencionar lo señalado, en su momento, mediante el oficio AD-ATIC-706-2020 del 16 de marzo 2020, respecto a los Plan de Continuidad de la Gestión en Tecnologías de Información, así como, el rol y responsabilidades de la Subárea de Continuidad de la Gestión, indicándose, lo siguiente:

> *(…) la Institución ha emitido manuales de organización y funciones en TIC que refieren sobre las actividades sustantivas correspondientes al tema de continuidad de servicios y otros afines, esto a partir de los procesos establecidos en cada nivel organizacional conformado, estableciendo ahí los roles y responsabilidades respectivamente, según se puede observar en la siguiente tabla:*

Tabla No.1
Actividades sustantivas establecidas en manuales de organización respecto a la continuidad de los servicios tecnológicos

Marco Normativo	Unidad encargada	Actividades sustantivas
Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones	*Área de Seguridad y Calidad Informática*	*-Verifica la continuidad de la gestión y los planes de contingencia*
Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones	*Subárea de Continuidad de la Gestión*	*-Participa en la formulación, la actualización y evaluación de la regulación y la normativa técnica.* *-Realiza investigación de carácter operativo.* *-Participa en la elaboración de carteles de licitación.* *-Documenta los procedimientos operativos en su ámbito de acción.* *-Propone políticas, estrategias, protocolos, estándares y procedimientos para garantizar la continuidad de la gestión.* *-Elabora planes de contingencia, de continuidad de la gestión y de recuperación de información en los diversos niveles de la organización.* *-Actualiza semestralmente los planes de contingencia.* *-Analiza y proponer acciones para evitar posibles riesgos en la operación de los sistemas y tecnologías de información y comunicaciones institucionales.* *-Coordina acciones con los centros de gestión informática* *-Genera cultura informática en su ámbito de acción.* *-Realiza pruebas y simulacros a nivel institucional.* *-Coordina actividades con los responsables de la operación de sistemas y tecnologías de información y comunicaciones a nivel institucional.* *-Aplicar las políticas y estrategias de seguridad y calidad* *-Asesora a las diversas unidades de trabajo en su ámbito de competencia.* *-Proporciona a la administración un sitio alterno para el procesamiento de información de los sistemas críticos institucionales.* *-Coordina con las entidades externas respectivas la comunicación eficaz en caso de emergencia.* *-Elabora planes de recuperación de información en casos de emergencia o desastres.* *-Proporciona un sitio alterno para la custodia y procesamiento de la información institucional crítica.* *-Seguimiento, control, evaluación y retroalimentación de la gestión.* *-Administración de los recursos.* *-Promoción de la cultura organizacional.* *-Implementación del sistema de control interno.* *-Participa en la formulación del plan operativo y del presupuesto.*

*"(…) **4. Sobre los planes de continuidad en TIC***

Se determinó oportunidades de mejora en torno a la integración de planes de contingencia en TIC que brinden procesos orientados a brindar continuidad a las operaciones en tecnologías de información y comunicaciones, con un enfoque de disponibilidad de herramientas digitales como medios alternativos, evitando dependencia hacia la resolución de incidencias por parte de otros niveles organizacionales, evidenciándose la falta de definición clara de los responsables y las acciones para responder a esos incidentes.

Por lo anterior, esta situación podría exponer la continuidad de las operaciones y servicios tecnológicos brindados en la Institución, sin mantenerse las condiciones idóneas y sobre todo limitando la adopción de soluciones integrales para la resolución de incidencias (…)

5. Sobre el rol y responsabilidades de la Subárea de Continuidad de la Gestión

Durante el análisis de las condiciones presentadas producto de la interrupción de servicios tecnológicos de la CCSS en octubre del 2019, este Ente Fiscalizador identificó la ausencia en la participación de la Subárea de Continuidad de la Gestión debido a que no se cuenta con ningún funcionario a cargo de los procesos llevados a cabo por el nivel organizacional supracitado.

Es importante considerar que dichas labores se encuentran definidas en el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones vigente, y están a cargo del Área de Seguridad y Calidad Informática con al menos 23 actividades sustantivas para obtener como producto final la continuidad de la gestión garantizada.

Al respecto, en oficio DTIC-0736-2020, suscrito por el Máster. Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones, indica lo siguiente sobre este tema:

"Actualmente, por motivo de acogerse en Abril 2019 al régimen de Pensiones IVM el funcionario encargado de dicha Subárea, en este momento no se cuenta con ningún funcionario encargado de la dicho proceso, desde finales del 2019 se están realizando las gestiones necesarias para activar la plaza de Jefe en Sistemas 1 de dicha Subárea y contar con un funcionario que brinde el seguimiento, gestión y control de la Continuidad de los servicios TIC, motivo por el cual, al momento de la incidencia del día 22 octubre, no hubo participación de ese personal(…)".

Con base en lo anterior, en consulta efectuada, el 20 de junio de 2022, a la Máster Vanessa Carvajal Carmona, jefe, Subárea Seguridad de Tecnologías de Información, Dirección de Tecnologías de Información y Comunicaciones, respecto a la carencia de un funcionario encargado de la Subárea de Continuidad de la Gestión, indicó:

"(…) la condición continua, no existe jefatura de la Subárea de Continuidad, y el único funcionario que estaba en esa subárea labora en mi subárea, y también ayuda a la jefatura de Área de Seguridad en algunos temas de Continuidad, pues el recargo de esa función la tiene la jefatura de Área".

2.3 De la información aportada por unidades institucionales, referente al impacto en la prestación de servicios y Planes de Continuidad en TIC:

Esta auditoria realizó consulta a 58 unidades institucionales (áreas de salud, hospitales y sucursales), sobre la existencia de un Plan de Continuidad de TIC (aprobado y actualizado) y su utilidad para atender la emergencia suscitada a partir del 31 de mayo del 2022, generando los siguientes resultados:

Respecto la existencia de un Plan de Continuidad de TIC (aprobado y actualizado), de las 58 unidades consultadas 8 (14%) unidades indicaron no disponer de este instrumento de contingencia.

Por otra parte, al consultarles sobre la utilidad del plan, para atender la emergencia tecnológica suscitada a nivel institucional, 36 (62 %) de las unidades indicaron su imposibilidad de aplicarlo o utilizarlo en la presente situación, señalando algunas de ellas, lo siguiente:

Cuadro 1
Utilidad del Plan de Continuidad de TIC, para atender
la emergencia tecnológica suscitada a nivel institucional
periodo de consulta del 6 al 15 de junio de 2022

Nombre de la unidad consultada	¿Le resultó útil el Plan de Continuidad de TIC para atender la emergencia suscitada a partir del 31 de mayo del 2022?
Hospital Monseñor Sanabria Martínez	En parte, justamente porque el documento se elabora en base a las acciones que se debe realizar a lo interno en el hospital, sin embargo, a lo externo se sale de nuestro alcance. Además, que el plan de contingencia que se tenía con EDUS no funcionó.
Área de salud de Guápiles	No abarca situaciones como la ocurrida.
Área de Salud Alajuela Norte	El plan de contingencia no es aplicable para un evento de este tipo.
Área de Salud Los Chiles	No fue funcional, el impacto fue muy grande, por lo general se respalda la información en el servidor, pero estos se vieron afectados.
Área de Salud Dr. Solón Núñez Frutos	No, esto debido al alcance de la emergencia que es a nivel global, nuestro plan es para atender emergencias locales.
Hospital de Los Chiles	Se encuentra desactualizado y no incluyó el tema de continuidad de servicios ante hackeos.
Sucursal Los Chiles	El plan diseñado es para periodos cortos, y el tema del hackeo al afectar los sistemas ha excedido la capacidad de respuesta.
Área de Salud Alajuelita	El plan estaba enfocado principalmente a fallas de conexión, sin embargo, esta emergencia ha tenido incluso la imposibilidad de utilizar los equipos.
Área de Salud Horquetas Río Frío	El plan a lo largo del tiempo funcionó para realizar el reemplazo de los equipos, pero para esta situación no, fue una situación reactiva porque esos planes no están diseñados para prevenir esta emergencia.
Sucursal CCSS Turrialba	En estas situaciones los planes no fueron efectivos pues un evento de esta magnitud no estaba contemplado en los planes locales.
Área de Salud de Turrialba	No por la magnitud de la emergencia si están deshabilitados todos los servidores centrales y no funcionan las aplicaciones.
Área de Salud Aserrí	Estaba en el servidor y el mismo está afectado, no se pudo disponer de él.

Sucursal de Desamparados	El jefe de Sucursal indica que no fue útil, ya que considera que no es útil para atender esta macro emergencia, solo valioso para extraer datos a nivel local.
Área de Salud Pérez Zeledón	No se tenía contemplada una situación como la actual.
Área de Salud Heredia Cubujuqui	No fue útil ya que todos los respaldos en servidores fueron infectados.
Área de Salud Tibás Uruca Merced	No, los procedimientos alternos de trabajo en caso de falla de los sistemas de información críticos, contiene el uso de equipo de cómputo y por ejemplo en el caso del EDUS, el uso del EDAC, por lo que los mismos no pudieron implementarse, ya que la afectación se dio directamente en el equipo informático.
Área de Salud Oreamuno-Pacayas-Tierra Blanca	No, porque la instrucción fue no encender equipos, motivo por el cual no se pudo activar ese plan de contingencia.
Sucursal Cartago	No, nuestro plan de continuidad aprobado no es para este tipo de eventos.

Fuente: Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

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

> *"Los Planes de Continuidad de la Gestión, deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.*
>
> *La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. Adicionalmente como los planes de continuidad de la gestión pueden fallar debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, debe considerarse dentro de su administración la realización de pruebas periódicas para garantizar que los mismos estén actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes".*

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

> *"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*

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

Según el marco referencial COBIT 5 (Objetivos de Control para las Tecnologías de Información), en la descripción del proceso DSS04, DSS04.02 y DSS04.04 se indica lo siguiente:

> *"establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa".*
>
> *"evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción".*
>
> *"probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera."*

IV. CONSIDERACIONES

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

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

En relación con lo anterior, en la Caja Costarricense de Seguro Social, las tecnologías de información y comunicaciones han representado un rol fundamental en las estrategias implementadas para mejorar la calidad y accesibilidad de los servicios a nuestros usuarios, asimismo, se han convertido en una herramienta primordial para el uso racional de los recursos y optimización de la gestión medica – administrativa; escenario que se ha visto afectado debido al contexto actual.

En virtud de lo expuesto y con sustento en la información recopilada por esta Auditoría, resulta necesario, dar particular atención a la situación (actual) de la Subárea de Continuidad de la Gestión, respecto a la carencia de una jefatura y personal exclusivamente dedicado a realizar las actividades sustantivas de dicha unidad, lo cual podría limitar el ámbito de acción o la cobertura establecida en el marco normativo institucional de TIC.

Así mismo, resulta necesario que, los diferentes actores involucrados: Dirección de Tecnologías de Información y Comunicaciones, Área de Seguridad y Calidad Informática, Subárea de Continuidad de la Gestión, Centros de Gestión Informática gerenciales, regionales y locales, entre otros; efectúen una revisión y análisis de la calidad y eficacia de la estrategia actual establecida en torno a los Planes de Continuidad de la Gestión de TIC (contingencias requeridas y capacidad de replicación), su alcance (establecimiento de riesgos y vulnerabilidades), actualización (con el objeto de reflejar siempre la realidad del entorno), políticas y procedimientos con referencia a la continuidad de las operaciones (para identificar las principales regulaciones nacionales e internacionales de aplicación en la materia), así como, de los procesos de respaldo de los sistemas informáticos y bases de datos, de modo que se garantice el cumplimiento de los objetivos institucionales establecidos y la continuidad de los procesos de salud, pensiones y recaudación patronal, según corresponda.

De conformidad con lo expuesto, y en apego al artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones que se ejecuten, resulta fundamental que la administración activa se mantenga vigilante de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias, a fin de garantizar razonablemente la recuperación y continuidad de los servicios en la gestión de Tecnologías de Información y Comunicaciones.

Asimismo, es importante que, en las acciones a ejecutar para dar continuidad a la prestación de los servicios, se implementen los mecanismos básicos de control, con el fin de garantizar la legalidad de las operaciones, igualmente, se acrediten documentalmente los lineamientos y directrices para orientar la gestión en TIC, así como la fundamentación de las decisiones que se adopten, y se mantenga la emisión de informes de rendición de cuentas a las autoridades superiores.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.14 16:48:25 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AEBB/lbc

Anexo(2)

1. Productos emitidos por la Auditoría Interna sobre Planes de Continuidad de la Gestión en Tecnologías de Información (nivel central).
2. Productos emitidos por la Auditoría Interna sobre Planes de Continuidad de la Gestión en Tecnologías de Información (nivel operativo o local)

C. Auditoría.

ANEXO 1

Cuadro 2
Productos emitidos por la Auditoría Interna sobre Planes de Continuidad de la Gestión en Tecnologías de Información (nivel central)

ASS-253-2010 “Informe referente a la evaluación del arriendo de un sitio alterno para resguardo de respaldos de información, DTIC”.
ATIC-336-2011 “Evaluación de los mecanismos para la administración de planes de continuidad de tecnologías de información y comunicaciones”.
ATIC-172-2013 “Evaluación sobre la gestión de planes de continuidad en tecnologías de información y comunicaciones en la Caja Costarricense de Seguro Social”.
ATIC-106-2017 “Gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de una contratación directa de servicios profesionales a la Firma Consultora Deloitte & Touche”.
Oficio AD–ATIC–8137–2018 “Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS”.
Oficio No. 9125 “Resultado informe denominado “Evaluación de carácter especial sobre la gestión efectuada en el cumplimiento de los planes remediales del Análisis Integral de Vulnerabilidades y Riesgos en TIC de la CCSS.
Oficio de advertencia AD-ATIC-706-2020 sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre 2019.
AD-ATIC-1512-2020 “Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio”.
AD-ATIC-706-2020 “Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre del 2019”.
AS-ATIC-2313-2021 “Oficio de Asesoría referente a mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas”.
AD-ATIC-038-2022 “Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo de 2022”.
AD-ATIC-039-2022 “Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS”.

ANEXO 2
Cuadro 3
Productos emitidos por la Auditoría Interna sobre Planes de Continuidad de la Gestión en Tecnologías de Información (nivel operativo o local)

AGO-093-A-2010 “Estudio referente a la implementación del Modelo de Organización de los Centros de Gestión Informática en la Dirección Regional de Sucursales Brunca”.
AGO-124-2010 “Evaluación de la seguridad lógica del Sistema Integrado de Farmacia (SIFA) en el Hospital de Upala”.
AGO-131-2010 “Evaluación de la seguridad física del Centro de Gestión Informática del Hospital La Anexión”.
ASS-201-2010 Evaluación referente a la seguridad física y lógica de las tecnologías de información y comunicaciones en el área de Salud Coronado”.
AGO-161-2011 “Cumplimiento del Plan de Continuidad de la Gestión en tecnologías de información y comunicaciones en el Hospital La Anexión”
AGO-346-2011 “Evaluación referente al Plan de Continuidad de la gestión en tecnologías de información y comunicaciones del Centro de Gestión Informática de la Dirección Regional de Servicios de Salud Brunca”.
AGO-352-2011 “Evaluación de la seguridad física y ambiental de los cuartos de telecomunicaciones del Hospital Los Chiles”.
AGO-314-2012 “Evaluación referente al Plan de Continuidad de la gestión en tecnologías de información y comunicaciones del Hospital Dr. Fernando Escalante Pradilla”.
AGO-144-2016 “Evaluación integral de la gestión médico – administrativa desarrollada en el Área de Salud Santa Cruz. Tema: Gestión de tecnologías de información y comunicaciones”.
AGO-17-2017 “Evaluación integral de la gestión médico – administrativa en el Área de Salud Mata Redonda – Hospital “Clínica Dr. Ricardo Moreno Cañas”, Tema: tecnologías de información y comunicaciones”.
AGO-66-2018 “Evaluación integral de la gestión médica-administrativa desarrollada en el Área de Salud Parrita, referente a las tecnologías de información y comunicaciones”.
AGO-97-2018 “Evaluación integral en la Sucursal Santa Cruz, respecto a la gestión de ingresos, egresos, seguridad física, infraestructura, incapacidades, perfiles de usuario y continuidad de los servicios”.

AGO-164-2018 “Auditoría de carácter especial sobre el control interno establecido para la gestión de las tecnologías de información y comunicaciones en el Área de Salud Chomes – Monteverde”.
AGO-219-2018 ““Evaluación integral en la Sucursal La Cruz, respecto a la gestión de ingresos, egresos, seguridad física, infraestructura, incapacidades, garantías de participación, ajustes de planillas y continuidad de los servicios”.
AGO-37-2019 “Auditoría de carácter especial sobre la gestión de tecnologías de información y comunicaciones en el Área de Salud Cariari”.
AGO-111-2019 “Auditoría de carácter especial sobre el control interno establecido para la gestión de las tecnologías de información y comunicaciones en el Área de Salud Esparza”.
AGO-170-2019 “Auditoría de carácter especial sobre el control interno establecido para la gestión de las tecnologías de información y comunicaciones en el Área de Salud Garabito”.
AGO-52-2020: “Evaluación sobre la implementación del Expediente Digital Único en Salud (EDUS) en los EBAIS adscritos al Área de Salud de Nicoya”.
AGO-85-2020 “Auditoría de carácter especial sobre el control interno establecido para la gestión de las tecnologías de información y comunicaciones en el Área de Salud Barranca”.
AGO-97-2020: “Auditoría de carácter especial referente a la aplicación ARCA en el Hospital San Carlos”.
AGO-78-2021 “Auditoría de carácter especial sobre la gestión de tecnologías de información y comunicaciones en la Dirección Regional de Sucursales Huetar Atlántica”.