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

AS-AATIC-088-2022
16 de junio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Doctor
Randall Alvarez 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 TECNOLOGÍA-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

Máster
Idannia Mata Serrano, subgerente a.i
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Estimados señores:

ASUNTO:	**Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y consecuente al oficio AI-874-2022 del 6 de junio del 2022, en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022, se advierte a esa Administración sobre la temática relacionada con la continuidad del negocio ante amenazas o desastres de origen tecnológico.

Lo anterior, al considerar el contexto actual de la CCSS, particularmente dando énfasis a los ataques cibernéticos recientes y que aún afectan la dinámica habitual de los procesos de negocio.

1. GENERALIDADADES Y ANTECEDENTES

1.1 Términos y definiciones

Para iniciar, se debe comprender que las organizaciones, dentro de su gestión de negocio (procesos) depende del soporte de la información y sistemas (tecnologías), entre otros factores operacionales, logísticos y financieros.

No obstante, esa estrategia es susceptible a cambios en el entorno, amenazas o desastres causantes de la paralización de un servicio o proceso esencial, esto por un periodo de tiempo que pone en peligro a la organización, recursos, imagen, entre otros.

En ese sentido, algunos ejemplos de amenazas o desastres de origen natural o humano son:

- Desastres de origen natural:
  - Fuego
  - Inundaciones
  - Hundimientos
  - Sismos o terremotos
  - Epidemias

- Desastres de origen humano:
  - Fallos energéticos
  - Terrorismo
  - Vandalismo
  - Cortes de comunicación
  - Huelgas
  - Problemas de acceso

Ante ello, existen prácticas y estrategias que impulsan la atención de las exigencias organizacionales al contrarrestar los efectos de la materialización de riesgos, tales como los antes indicados.

En virtud de lo anterior, conviene comprender el significado del término supracitado y en segunda instancia percibir la relación que tiene con las Tecnologías de Información y Comunicaciones (TIC's), a saber:

En la página web de la empresa estadunidense VMware® (experta en soluciones transformación digital) se puede observar en el apartado de glosario, el significado correspondiente al término de **continuidad del negocio**, citando:

> *"es el nivel de preparación que tiene una empresa para mantener las funciones esenciales tras una emergencia o una interrupción. Estos eventos pueden incluir vulneraciones de seguridad, desastres naturales, cortes de energía, averías de los equipos o la salida repentina de un empleado clave".*

Es decir, se refiere a la capacidad estratégica y táctica de la organización para planificar y responder a incidentes o interrupciones, esto con el fin de continuar sus actividades de negocio bajo un nivel de subsistencia aceptable y previamente definido.

Para tales efectos, la continuidad de los procesos de negocio incluirá un conjunto de medidas contingenciales que le permitan a la entidad disminuir la afectación en sus actividades, mientras se vuelve a la situación inicial. Particularmente, al documentar estas acciones, se conforma el **"plan de continuidad del negocio"**, el cual contendrá a su vez un cierto número de planes diferentes, cómo el de evacuación, emergencias, gestión de incidentes, comunicaciones, contingencia de las TIC, seguridad de la información, entre otros.

A grandes rasgos, 3 son los elementos característicos de un plan de continuidad negocio, según lo describe el articulo “Contingencia TIC vs Continuidad de negocio”, publicado el 30 de setiembre del 2011 por el Instituto Nacional de Ciberseguridad (INCIBE) de España, citando:

> *“-Garantiza la continuidad de los procesos ante desastres y eventualidades.*
>
> *-Es un elemento estratégico global que se sustancia de n planes de contingencia de áreas de negocio y n planes de contingencia de las infraestructuras en las que soporta el negocio, entre ellas los sistemas de información y comunicaciones.*
>
> *-Tiene como objetivo dar respuesta a las situaciones que no han podido ser evitadas por las medidas de seguridad implementadas por la organización.”*

1.2 Contexto institucional

El 31 de mayo del 2022 se dio a conocer un nuevo hackeo, según la publicación del diario “La Nación”, titulado “Nuevo ‘hackeo’ en CCSS afecta atención en hospitales y EBAIS por desactivación del EDUS”, a saber:

> *“La Caja Costarricense de Seguro Social (CCSS) sufrió un nuevo hackeo la madrugada de este martes 31 de mayo, el cual obligó a desactivar todos los sistemas informáticos de la entidad de manera preventiva (…)”*

Ese mismo día, las autoridades de la Caja Costarricense de Seguro Social (CCSS) informan formalmente a la prensa que el hackeo registrado fue “excepcionalmente violento” y el Dr. Alvaro Ramos Chaves, presidente ejecutivo de la Institución, hizo el siguiente llamado ante la situación de marras, citando:

> *“Pedimos paciencia porque tenemos mucho trabajo por delante. La gente razonablemente se ha acostumbrado a la agilidad con la que podemos hacer las cosas cuando tenemos recursos digitales, pero tendremos que recurrir por unos días al papel. Este fue un intento muy violento de vulnerar bases de datos, los sistemas de la Caja, tenemos que pedir paciencia en ese sentido.”*

En línea con lo anterior, el Dr. Ramos insistió en que no fueron los hackers los que cerraron las bases de datos ni apagaron los sistemas, mencionando la medida tomada a nivel interno de la CCSS:

> *“Fuimos nosotros mismos, eso que quede muy claro, para que los hackers no pudieran acceder a ella. Naturalmente no tenemos certeza absoluta de que no haya exfiltración de una parte parcial de estos datos, pero estamos bastante confiados en que no fue así. Nuestros datos preliminares es que no pudieron sacar esa información, con una investigación profunda terminaremos de saberlo con certeza.”*

No obstante, el 2 de junio del 2022, se dio a conocer la noticia “‘Hackers’ infiltraron la CCSS desde febrero” publicada por el diario la Nación, donde se amplía con mayor precisión la afectación dada en el equipo tecnológico de la CCSS y la eventual respuesta al restablecimiento de los servicios, citando:

> *“Todos los indicios apuntan a que los hackers empezaron a gestar su ciberataque a los sistemas de la Caja Costarricense de Seguro Social (CCSS) desde febrero, pues, desde ese mes, en la llamada Internet oscura (”dark web”), comenzaron a ofrecer accesos a los sistemas informáticos de la entidad, reveló el presidente ejecutivo, Álvaro Ramos Chaves, al admitir que el daño es mayor al que calcularon el martes.*
>
> *Se sospecha que el “software” hostil que inyectaron los extorsionadores entró por alguna terminal o computadora y logró infectar a otras 9.000 (22%) de las 40.000 unidades que tiene la institución. También logró penetrar no a 30, como se dijo inicialmente, sino a 800 servidores (53%) de los 1.500 que tiene la CCSS y, ya una vez adentro, asestó el zarpazo final este 31 de mayo cuando se activó y alteró los sistemas.*

(…) "Los técnicos, no necesariamente de la Caja, me han estado informando de que, por ejemplo, hay evidencia en lo que llaman las redes oscuras de que había actores conocidos en ese tipo de redes ofreciendo accesos a la Caja, y que posiblemente hubo múltiples intentos de acceso (…) Ahora que se hace la revisión forense en la dark web encuentran que había gente ofreciendo (información)", explicó.

Admitió que, desafortunadamente, la dimensión del daño es mayor a la que se dijo en un inicio. No se atrevió a dar un plazo para restablecer todos los sistemas, aunque espera que el Expediente Digital Único en Salud (EDUS), en su versión de respaldo para situaciones de emergencia –conocido como EDUS desconectado– pueda estar disponible en no menos de una semana."

En síntesis, la CCSS fue expuesta a un incidente de ciberseguridad, el cual desencadenó la paralización de componentes tecnológicos y se afectó el funcionamiento usual de los servicios de salud, pensiones y prestaciones sociales.

1.3 Productos emitidos recientemente por la Auditoría Interna

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

A ese respecto, en la siguiente tabla se observan los productos recientes que abordan la temática supracitada de manera concreta.

Cuadro No.1
Productos emitidos Auditoría Interna sobre continuidad del negocio y contingencia de servicios TIC

Informe / Oficio No.	Fecha	Asunto
Oficio AD-ATIC-706-2020	16 de marzo, 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.
AD-ATIC-1512-2020	29 junio de 2020	Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio.
AD-ATIC-038-2022	21 de abril del 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.
AS-AATIC-072-2022	10 de junio del 2022	Oficio Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.

Fuente: elaboración propia

Adicionalmente, este Ente Fiscalizador se ha pronunciado de manera constante sobre temas interrelacionados, por ejemplo: las condiciones y oportunidades del sitio alterno, mecanismos para la administración de planes contingenciales TIC, gestión de la continuidad del negocio, fortalecimiento de la plataforma tecnológica, seguridad informática y de la información, telecomunicaciones, tendencias tecnológicas, gobernanza de las TIC, cumplimiento de marco normativo, entre otros asuntos de vital relevancia.

1.4 Consideraciones normativas

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

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

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

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

> *"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
>
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."*

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

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

Según el marco referencial COBIT 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.".

2 OBSERVACIONES

Así las cosas, esta Auditoría Interna se refiere al argumento citado en el epígrafe, con el objetivo de que esa Administración defina estrategias ante los eventos recientes y venideros. Lo anterior, dada la importancia que reviste la continuidad del negocio y el impacto ocasionado a raíz de los ataques cibernéticos perpetrados a nivel institucional y posiblemente reiterativos.

En ese sentido, se hace de su conocimiento las siguientes observaciones para su valoración:

2.1 Establecimiento de un sistema de gestión de la continuidad de negocio

Las organizaciones modernas apuntan a establecer formalmente un Sistema de Gestión de la Continuidad del Negocio (SGCN) estructurado y socializado, con el objetivo de permitir obtener una ventaja propia y ante terceros de recuperarse pese a un evento y/o incidente que cause interrupciones considerables en la cadena de producción o de negocio.

Lo anterior, ante una legislación y requerimientos de negocio que demandan una capacidad estratégica y técnica de la organización para prepararse proactivamente frente a contingencias o interrupciones de todo tipo, e inclusive presumiendo diferentes niveles de gravedad, según la importancia del ámbito donde se pueda producir el paro o inactividad.

En ese sentido, la excepción no es la CCSS y de diseñarse e implementarse correctamente dicho sistema, se obtendrían beneficios de valor agregado. A ese respecto, según EALDE (escuela española de negocios Online para Directivos) en su blog "ISO 22301: Cómo establecer un Sistema de Gestión de Continuidad del Negocio" publicado el 6 de enero del 2021, cita las siguientes ventajas de establecer el sistema supracitado:

"-Mejora de la gestión de los riesgos empresariales.
-Reconocimiento por parte de proveedores y clientes.
-Solidez empresarial, que servirá para afrontar cualquier tipo de emergencia o suceso que pueda ocurrir.
-Ahorro en costes y tiempo, al tener estudiada una respuesta ante interrupciones de la actividad."

2.2 Oportunidad de los mecanismos de contingencia que buscan brindar continuidad al negocio

Observando el comportamiento de la Institución al generar soluciones que compensen la ausencia de equipo tecnológico y sistemas de información, resalta la necesidad de valorar la efectividad, suficiencia y oportunidad de las acciones contingenciales.

En ese sentido, recordando que el plan de contingencia se enmarca como parte de la gestión de continuidad y tratamiento del riesgo en la organización; por ello, este debe ser implementado mediante un ciclo de mejora continuo con la premisa de admitir la incorporación y evaluación de elementos asociados con la definición de las situaciones críticas, asignación de responsables, determinación de acciones de respuesta y el mantenimiento de los procedimientos establecidos.

Lo anterior, para que pueda calificarse como suficiente, óptimo y efectivo, así mismo, ofreciendo la respuesta a la pregunta ¿qué hacer para revertir la situación de crisis una vez producida? Es decir, evitando imprecisiones o márgenes de error que provoquen la materialización de otros riesgos.

Particularmente, el plan de continuidad del negocio y de contingencia TIC efectivo, podría detallar los mecanismos que aplican ante un incidente, tal como el acontecido recientemente en la CCSS, el cual es de origen cibernético e inclusive plasma de forma planificada las acciones a seguir contemplando la limitante de utilizar la red de datos, sistemas de información, equipo de cómputo, entre otras casuísticas del entorno.

A manera de ejemplo, se expone las siguientes noticias que refieren a la oportunidad de los mecanismos de contingencia, definidos para garantizar la continuidad del negocio, a saber:

- Publicación "'CCSS corre para montar sistema de pago de incapacidades generadas después de 'hackeo'" del 8 de junio del 2022, por parte del diario La Nación, en la cual cita:

  "Estamos trabajando en un mecanismo alterno para pagar las (nuevas) incapacidades que se han generado en estos días. Los centros médicos siguen generando incapacidades, pero ahora de manera física (en papel)", manifestó Picado."

- Publicación del 11 de junio del 2022 del periódico "El Coronadeño Hoy" en su perfil de Facebook, en la cual se cita la condición del mecanismo de contingencia para efectuar llamadas al Área de Salud de Coronado y su eventual limitación, a saber:

  "¿Está funcionando la central telefónica?
  Con respecto a las quejas en ese sentido, de gente que dicen que llaman y no les contestan, quiero aclarar que tenemos una central telefónica IP, lo que significa que la central está en un computador. Entonces, en este momento no hay central telefónica y por lo tanto hay una persona atendiendo el teléfono, lo que genera una cola muy grande de llamadas, algunos se esperan otros no, esperamos restablecer muy pronto la normalidad en este servicio."

- Publicación "'Hackeo' a CCSS: farmacias elevan control a recetas por gente que pide más medicinas de la cuenta" de fecha 13 de junio del 2022, por parte del diario La Nación, en la cual cita:

  "El ciberataque del 31 de mayo dejó a todos los servicios de salud trabajando a pie. Las farmacias no han sido la excepción y se han visto obligadas a llevar el control del despacho de medicinas a mano. Esta situación fue aprovechada por gente que, ante la falta de expediente digital que facilite la información médica del paciente, pide más de lo que necesita y se aprovecha de la dificultad de los centros para corroborar 'a pie' los tratamientos de los asegurados.

  Según informó la entidad, algunas farmacias han reportado el retiro de medicamentos por encima del promedio usual, lo cual les hace sospechar que algunas personas pueden estar retirando más medicinas de las necesarias. Esto también aumenta el riesgo del abuso o del buen manejo de los fármacos."

- Publicación del diario Semanario Universidad "Centros de Informática de seis hospitales de la Caja están "limitados" para dar respuesta en ciberseguridad" de fecha 14 de junio del 2022, la cual menciona:

  "Los Centros de Gestión Informática locales de seis hospitales de la Caja Costarricense de Seguro Social (CCSS) señalan estar "limitados" en cuanto al desarrollo de ciberseguridad. Así lo dejaron claro estas dependencias en un oficio enviado a la Dirección de Tecnologías de Información y Comunicaciones el pasado 7 de junio.

  "El rol de los Centros de Gestión Informática locales se encuentra limitado en tiempo, respuesta, y soluciones, esto en razón de que los distintos elementos en materia de seguridad informática, todos relacionados con las buenas prácticas a implementar para la protección de la información, a fin de prevenir, detectar y detener posibles ataques cibernéticos, son de control estricto y exclusivo de la dirección a su cargo, por parte del Área de Seguridad y Calidad Informática", externaron los Centros.

En la comunicación, esta dependencia agregó que al ser esos elementos palanca del Área de Seguridad y Calidad Informática, la dotación institucional de recursos tanto humanos, técnicos, como financieros se limita a dicha área, y no a sus centros locales, quienes más bien tienen faltantes."

Por todo lo anterior, se debe recordar que los mecanismos de contingencia deben ser funcionales y minimizar de manera considerable el impacto y/o efecto ante una amenaza o desastre.

2.3 Estandarización de medidas y consolidación de esfuerzos

Con el objetivo de brindar un adecuado direccionamiento sobre la línea a seguir en cuanto mecanismos de contingencia, las medidas deben ser examinadas, aprobadas y estandarizadas por las estructuras correspondientes.

En ese sentido, evitando la resolución a criterio o ingenio de la parte operativa y buscando un proceso ordenado para la atención a la emergencia; Lo anterior, por medio de la participación de los responsables en el nivel estratégico, especialistas técnicos, asesores legales, entre otros funcionarios que generan sus aportes en relación con las necesidades consolidadas y buscan establecer soluciones o alianzas transversales a la organización.

Algunos ejemplos de publicaciones de diarios a nivel nacional que refieren a esa temática son:

- Nota periodística "Máquinas de escribir, Excel y WhatsApp, entre los aliados anti-'hackeo' de Ebáis y hospitales" de fecha 12 de junio del 2022, publicada por el diario La Nación, citando:

  "Las tres máquinas de escribir que servían de adorno en los estantes de la Farmacia del Área de Salud de Garabito, en el Pacífico Central, fueron desempolvadas para escribir las etiquetas que ya no se pueden generar digitalmente, después del hackeo a la Caja Costarricense de Seguro Social (CCSS).

  (…) "A pesar de estos métodos alternativos no dábamos abasto con la cantidad de recetas. Posteriormente, empezamos a utilizar una herramienta en Excel para agilizar el proceso para que fuera más claro para el paciente el mensaje y, poco a poco, hemos ido saliendo con la consulta", cuenta Rodríguez.

  La famosa hoja de datos les ha salvado la tanda. En Garabito usan una desarrollada por el farmacéutico Armando Sánchez, del área de salud de Parrita, que les ha servido como plan de contingencia para el despacho de los medicamentos en la Red Integrada de Prestación de Servicios de Salud Pacífico Central.

  (…) Herramientas como la mensajería por WhatsApp también se han vuelto indispensables. Por esa vía, por ejemplo, los Ebáis desconcentrados envían los datos del paciente y del medicamento que necesita para que se lo despachen al día siguiente. Esto ha permitido que enfermos crónicos, como diabéticos e hipertensos, cuenten con su tratamiento."

Aunado a ese riesgo, se ha de considerar el contexto institucional contra las condiciones atinentes a las soluciones de uso individual y/o personal de los funcionarios, por ejemplo, al utilizar aplicaciones de mensajería instantánea, repositorios en la nube, gestión de llamadas o datos, entre otras.

2.4 Definición de valores críticos

Basado en las mejores prácticas concernientes al tema, la organización debe establecer y monitorear los valores críticos que le permitan evaluar sus necesidades en cuanto a brindar continuidad a los procesos y planificar su recuperación.

Para tales efectos, se define brevemente los valores supracitados, a saber:

- MPTB (Periodo Máximo Tolerable de Interrupción) periodo máximo sin el funcionamiento de un proceso o servicio, sin poner en peligro la supervivencia de la organización.
- RTO (Objetivo de Tiempo de Recuperación) periodo máximo de tiempo que puede pasar desde el momento del incidente hasta ser recuperado. Es decir, está ligado con el tiempo de recuperación y se trata de un lapso menor al MPTB.
- OPT (Objetivo de Punto de Recuperación) es el punto en que los recursos (humanos, tecnológicos, logísticos, entre otros) han quedado restaurados y permite el desarrollo de actividades.

Estos indicadores apoyarían el objetivo de identificar los umbrales establecidos en los diferentes procesos en la organización; cuánto tiempo podrían estar paralizados y consecuentemente activar las estrategias destinadas para atender la operación crítica, entorno TIC, entre otras áreas; todo lo anterior, de forma priorizada, secuencial y considerando el respectivo tratamiento para cada enfoque.

2.5 Marco normativo y guías desde el ámbito de negocio y tecnológico

Sobre el cumplimiento del marco normativo, es relevante que esa Administración pueda verificar el apego a este, así como la capacidad y oportunidad de lo referido, esto en atención al contexto actual de la Institución y considerando las variables del entorno. A ese respecto, analizando al menos lo dispuesto en la norma citada a continuación.

- Ley y Normas de Control Interno para el Sector Público.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021.
- Normas Institucionales de Tecnologías de Información, CCSS.
- Políticas Institucionales de Seguridad Informática, TIC-Seguridad-001, Versión 1.0 de octubre 2007.
- Normas Institucionales de Seguridad Informática, TIC-ASC-SEG-0002, Versión 1.0 de abril 2008.

Por otra parte, se puede enfatizar, la atención en el conjunto de buenas prácticas, que detallan recomendaciones a valorar para coadyuvar al fortalecimiento de las labores asociadas con la sustentabilidad del negocio en materia de la información, aplicaciones informáticas, cuestiones financieras, contables y legales, así como también los procesos productivos y operativos.

Para tales efectos, se mencionan algunos marcos de referencia y normas ISO asociados a la temática expuesta:

- Estándar ISO 22301 Sistema de Gestión de la Continuidad del Negocio.
- Norma de Gestión de Seguridad de la Información ISO/IEC 27001, 27002.
- ISO 20000 Sistema de Gestión de Servicios de Tecnologías de la Información.
- Marco referencial COBIT 5 (Objetivos de Control para las Tecnologías de Información).
- Marco de ciberseguridad NIST (acrónimo de Instituto Nacional de estándares y tecnología, en inglés).
- Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) considerada como una guía de buenas prácticas para la gestión de servicios de TI.

Lo anterior, sabiendo que el marco normativo y demás documentos buscan apoyar la necesidad de regular y/o guiar el adecuado ejercicio de labores o comportamientos deseables en la organización para mantener el orden, articular esfuerzos, entre otros propósitos que pueden resultar valiosos e inclusive la cura para temas particulares.

2.6 Estructura de fases y utilización de recursos

Según los marcos de referencia en materia de sostenibilidad del negocio, la materialización de riesgos ocasionados por amenazas o desastres debe ser inclusiva a la participación del nivel estratégico y táctico para tomar decisiones y mantenerse vigilante al cumplimiento de fases atinentes al plan de continuidad, esto en aras de buscar un proceso ordenado desde que se materializa el riesgo, su tratamiento progresivo y consecuentemente el restablecimiento de servicios (funcionamiento habitual de la organización).

En ese sentido, ese comportamiento podría imitarse en la CCSS, a fin de disponer de un ciclo ordenado que normalice la activación de protocolos; análisis de impacto y riesgo; definición de estrategias y alianzas; desarrollo e implantación de planes; pruebas y evaluación de acciones; restablecimiento paulatino y secuencial; y finalmente su mantenimiento o mejora en atención a lecciones aprendidas o necesidades específicas.

Todo lo anterior, considerando la gestión de recursos en materia de personas, tecnologías, tiempos, información, documentación, ubicación, comunicaciones, mecanismos de control, entre otras áreas.

A ese respecto, dando énfasis en la identificación concisa y objetiva de actividades, roles y responsabilidades enfocadas en atender lo correspondiente a la emergencia, así como validar el cumplimiento de normas; actualización del marco regulatorio; desarrollo de iniciativas asociadas con la continuidad del negocio; entre otras recomendaciones inmersas en esta misiva.

2.7 Gestión de crisis

Pese a considerarse la gestión de la crisis parte del plan de continuidad del negocio en una organización, se hace énfasis en la importancia de atender lo correspondiente como un elemento diferencial en mitigar el caos o confusión por medio de directrices claras y la habilitación de mecanismos de comunicación.

A ese respecto, esta Auditoría emitió del producto AS-AATIC-072-2022 del 10 de junio del 2022, en el cual detalló los aspectos concernientes a la gestión de crisis, esto al indicar la premisa institucional para elaborar un plan de crisis; habilitar estructuras y habilidades; monitorear las acciones implementadas, planificación de labores a ejecutar a nivel estratégico, táctico y operativo; gestionar la comunicación, entre otros elementos claves.

3 CONSIDERACIONES FINALES

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

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

Por ello, resulta fundamental el significado de la continuidad del negocio y en segunda instancia lo correspondiente a los mecanismos de contingencia de las áreas técnicas que brindan apoyo a los diferentes procesos.

Particularmente, siendo consecuentes con el contexto actual del ciberataque sufrido en la CCSS, donde fue evidente que se pusieron en marcha algunos planes de contingencia y probablemente otros carecieron de efectividad al pretender ser aplicados en las diferentes unidades de trabajo, pero más allá de eso es la oportunidad de incentivar la planificación, inversión y fortalecimiento de los planes de continuidad y contingencia a nivel institucional.

No obstante, se previene a esa Administración sobre lo indispensable que resulta la adopción de un plan de continuidad del negocio, debidamente integrado y con mecanismos de contingencia oportunos; basado la estandarización de soluciones, identificación de valores críticos, aplicación de normas y metodologías oficializadas en la institución; así como valorando lo indicado en marcos referenciales de buenas prácticas que permitirían construirlo, ponerlo en marcha o perfeccionarlo.

Sobre el particular, garantizando razonablemente la ejecución de acciones articuladas, bajo estructuras, roles, responsabilidades y habilidades que atiendan la gestión de continuidad y/o crisis desde la óptica de disponer de soluciones holísticas, directrices claras y enfocadas a mitigar de forma ordenada la interrupción de procesos o servicios.

En otras palabras, a partir del valor agregado que pueda generar el accionar de la Administración Activa para la implementación de las oportunidades de mejora expuestas en esta misiva.

De esa manera, marcando la diferencia para futuros incidentes en cuanto no perjudicar las actividades sustantivas, disminuir el daño de la imagen institucional o en caso de materializarse el riesgo prever de forma planificada una solución acorde a las necesidades del negocio y contexto del entorno.

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio, con el objetivo de evitar caos y confusión en cada una de las acciones a realizar como parte de la estrategia asociada con garantizar la continuidad del servicio; gestión de involucrados; plan de comunicaciones y otras actividades interrelacionadas a la temática.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.22 10:03:36 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/ghc

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva -1102
Ingeniera Susan Peraza Solano, directora, Dirección de Planificación Institucional-2902
Auditoría