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

AS-AAO-142-2022
11 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

Licenciado
Luis Fernando Campos Montes, gerente
GERENCIA ADMINISTRATIVA – 1104

Lic. Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA – 1103

Ing. Jorge Granados Soto, gerente
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍA - 1107

Lic. Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES - 9108

Dr. Esteban Vega de la O, gerente
GERENCIA DE LOGÍSTICA - 1106

Estimados señores:

ASUNTO:	**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.**

En cumplimiento del programa de actividades especiales consignado en el Plan Anual Operativo 2022 de esta Auditoria, y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se procede a informar a esas gerencias, aspectos relacionados con la cultura de administración del riesgo a nivel institucional y la simplificación de trámites y mejora regulatoria, en el contexto del ciberataque suscitado en la CCSS el 31 de mayo 2022.

Al respecto, esta Auditoría realizó una sesión de trabajo el 29 de junio 2022, con el Lic. Sergio Chacón Marín y la Licda. Andrea Zúñiga Chacón, director y jefa del Área de Gestión de Control Interno de la Dirección de Sistemas Administrativos, unidad adscrita a la Gerencia Administrativa, con el objetivo de conocer los principales riesgos identificados producto del ataque cibernético que sufrió la institución el pasado 31 de mayo 2022. Los resultados se enumeran en los siguientes apartados:

1. Sobre la administración y gestión de los riesgos institucionales

Según la norma internacional ISO 31000:2018 denominada Administración/ Gestión de Riesgo, la evaluación del riesgo tiene 3 componentes: identificación, análisis y valoración. Los primeros dos se realizan por medio de la elaboración de una matriz de riesgos, la cual ha sido establecida a nivel institucional, a través de la "*Herramienta de Gestión de Riesgos*", instrumento que orienta a la administración activa para definir las características del riesgo. Por otra parte, la valoración del riesgo se realiza a través de los mapas de calor, que tienen como propósito dictaminar y visualizar el tratamiento que se aplicará al riesgo.

En adición, la norma internacional antes descrita, en el apartado 6.5 expone las generalidades a considerar en el tratamiento de los riesgos en los siguientes términos:

> *"...El propósito del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos. El tratamiento de los riesgos implica un proceso iterativo de:*
>
> *— formular y seleccionar opciones para el tratamiento de los riesgos;*
> *— planear e implementar el tratamiento de los riesgos;*
> *— evaluar la efectividad de dicho tratamiento;*
> *— decidir si los riesgos residuales son aceptables;*
> *— si no son aceptables, efectuar algún tratamiento adicional..."*

En ese mismo apartado, la ISO:31000:2018, respecto a las opciones para el tratamiento de los riesgos indica:

> *"...Las opciones de tratamiento de los riesgos no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar los riesgos pueden implicar una o más de las siguientes:*
>
> *— evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo mismo;*
> *— aceptar o aumentar el riesgo en busca de una oportunidad;*
> *— eliminar la fuente de riesgo;*
> *— modificar la probabilidad;*
> *— modificar las consecuencias;*
> *— compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);*
> *— retener el riesgo con base en una decisión informada..."*

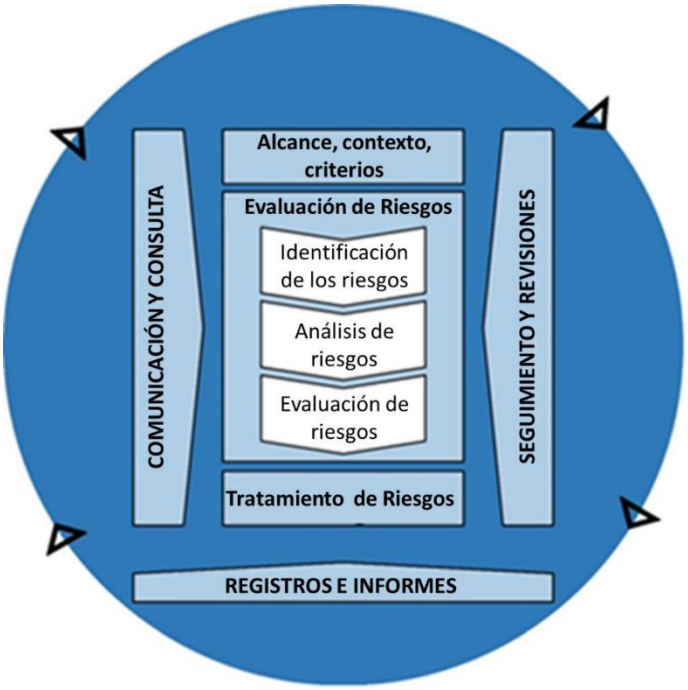
Explicado lo anterior, llama la atención que a nivel institucional para el año 2022, las unidades ejecutoras al efectuar la evaluación de los riesgos que pueden afectar la gestión, refieran a riesgos relacionados con los sistemas de información, en el siguiente cuadro se detallan, así como la frecuencia con que fueron expuestos:

Riesgos TI 2022	Frecuencia
TI-01	
TI-01 Falla en los sistemas informáticos	345
TI-02	
TI-02 Falla en la conectividad de los sistemas de información	276
TI-03	
TI-03 Acceso a información digital por parte de personas no autorizados	47
TI-04	
TI-04 Funcionario no tiene accesos a los sistemas informáticos requeridos	97
TI-05	
TI-05 Pérdida de información digital	322
Total referencias	**1087**

Lo anterior, muestra que en las unidades institucionales se identificó y analizó la posibilidad de una afectación de los riesgos asociados a las tecnologías de información y comunicaciones, no obstante lo anterior, es importante reflexionar acerca de cómo optimizar e interiorizar los procesos posteriores relacionados con el tratamiento, seguimiento y evaluación de esos potenciales riesgos, a través de las buenas prácticas emanadas en la ISO:31000:2018, lo anterior debido al grado de afectación en la institución ante el evento de ciberataque sufrido, aspecto importante en razón de que el resultado de una evaluación integral del riesgo, permite una toma de decisiones eficiente y el diseño de estrategias a implementar para mitigar o establecer planes de contingencia en caso de que éstos se materialicen.

Para un mejor entendimiento de lo anterior, vale la pena mostrar la siguiente imagen la cual permite una mejor visualización del proceso de administración de riesgos, de forma integral:

Imagen 1, Proceso de Administración/ Gestión de Riesgos



Fuente ISO:31000:2018

Nótese de la imagen anterior, que el proceso integral de gestión de riesgos involucra la definición de criterios, la evaluación de los riesgos (identificación, análisis y evaluación), el tratamiento y finalmente la elaboración de informes, que permitan posteriormente el seguimiento y revisión permanente.

La Contraloría General de la República emitió en el año 2005 las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos Institucional, y específicamente el apartado 4.5. sobre la administración del riesgo requieren que las Instituciones Públicas, efectúen las siguientes acciones:

> *"...**Administración de riesgos.** A partir de la priorización de riesgos establecida, se debe evaluar y seleccionar la o las medidas para la administración de cada riesgo, de acuerdo con criterios institucionales que deberán contener al menos los siguientes:*

a) la relación costo-beneficio de llevar a cabo cada opción;
b) la capacidad e idoneidad de los entes participantes internos y externos a la institución en cada opción;
c) el cumplimiento del interés público y el resguardo de la hacienda pública; y
d) la viabilidad jurídica, técnica y operacional de las opciones.

Se deberá valorar medidas dirigidas a la atención, modificación, transferencia y prevención de riesgos. En los casos en que sea imposible utilizar este tipo de medidas o las disponibles impliquen un costo mayor a su beneficio, la administración podrá retener dichos riesgos.

Las medidas para la administración de riesgos seleccionadas deberán:
a) Servir de base para el establecimiento de las actividades de control del sistema de control interno institucional.
b) Integrarse a los planes institucionales operativos y planes de mediano y largo plazos, según corresponda.
c) Ejecutarse y evaluarse de forma continua en toda la institución.

Lo descrito en el punto anterior, reafirma que la gestión de riesgos es un tema relevante y estratégico, en constante revisión, mejora y optimización, de ahí la necesidad que la Caja Costarricense de Seguro Social, centre su atención en mejorar estos procesos para disponer de una oportuna capacidad de respuesta ante la materialización de eventos que puedan tener un impacto severo en la gestión y consecución de los objetivos de la organización.

2. Cultura de la administración de la gestión de riesgos a nivel institucional

En esta misma línea de ideas, esta Auditoría ha señalado en sus informes respecto a la necesidad de revisar la metodología de valoración de riesgos, a fin de que se facilite la identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales relevantes, así como, informar al jerarca en relación con el estado de implementación del Sistema Específico de Valoración de Riesgos (SEVRI). Igualmente, se sugirió el establecimiento de lineamientos de monitoreo y seguimiento en relación con la administración de riesgos. (Informes de auditoría ASAAI-430-2015, ASAAI-136-2018).

Sobre estos aspectos, es importante traer a colación que el marco de gestión de Riesgos COSO-ERM-2017, se desarrolla a través de 20 principios que representan lo que las instituciones deberían hacer como parte de sus prácticas ERM (Gestión Empresarial del Riesgo), y específicamente para el fortaleciendo de la cultura de riesgos, plantea iniciativas mínimas necesarias para fortalecimiento de la cultura, según el siguiente detalle:

- *"...Asegurar que la Política de Riesgos de la entidad explicita los principios fundamentales de actuación ERM y que estos están alineados con los principios éticos plasmados en el Código Ético de la organización.*
- *Implementar iniciativas de comunicación y formación de los principios clave de ERM.*
- *Establecer un programa de objetivos e incentivos que fomente la interiorización de los principios de ERM, asegurando que los objetivos individuales están alineados con los objetivos estratégicos globales.*
- *Promover una cultura gerencial que incentive discusiones abiertas de los riesgos de la organización y promueva la toma de decisiones alineada con la cultura de riesgos seleccionada.*
- *Establecer programa de monitorización del cumplimiento con los valores clave ERM y divulgación de las medidas disciplinarias por su incumplimiento...".*

Las Normas para la gestión y control de las tecnologías de información del MICIT indican:

> *"IV. GESTIÓN DE RIESGOS TECNOLÓGICOS La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable. La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución".*

Derivado de lo anterior, resulta relevante para efectos de la situación experimentada por la institución en el contexto del ciberataque, la necesidad de fortalecer la cultura de riesgos a todo nivel de la entidad, así como la posibilidad de adoptar buenas prácticas de gestión del riesgo, como las establecidas en la norma ISO:31000:2018 y el marco de control COSO-ERM-2017, las cuales sin duda contribuirían para disponer de un mejor nivel de preparación y respuesta ante eventos no deseados.

El Lic. Sergio Chacón Marín, director de la Dirección de Sistemas Administrativos, externó ante la Auditoría que cuando se materializa el riesgo, los niveles operativos, en múltiples ocasiones, manifiestan que la responsabilidad de actuación es del nivel central o de un tercero, siendo éstos actores, como primera línea de defensa, los responsables de implementar las medidas de control, además, agregó que parte de las funciones de esa dirección, es promover las metodologías y el uso de los mecanismos que corresponden para que las unidades los apliquen y, la responsabilidad de implementar las medidas necesarias, de conformidad con los resultados de las herramientas, es de los titulares subordinados de cada unidad ejecutora.

En ese mismo orden de ideas, mencionó que los niveles operativos registran la información y pueden estar identificando los riesgos, pero el ejercicio de validación gerencial, de corroboración y de acción institucional de carácter estratégico no necesariamente es un proceso que esté fortalecido.

Como ejemplo, el Lic. Chacón comentó respecto a la enfermedad del COVID-19 que, conociendo –desde el año 2019- su origen y disponiendo de información internacional al respecto, muy pocas unidades -en el ámbito médico- consideraron -en sus mapas de riesgo- la posible afectación ; además, agregó que, por ejemplo, para el ataque cibernético que sufrió la institución el pasado 31 de mayo, estimó que un 3 % de las unidades adscritas a la Gerencia Médica, identificó los riesgos asociados a tecnologías de información y comunicaciones.

La situación descrita, corrobora aún más la necesidad de continuar incentivando la cultura de riesgos en la Institución, con el involucramiento de todos los actores, tanto en el nivel estratégico, como operativo.

3. Sobre la simplificación de trámites en el contexto del ciberataque

Referente al proceso de simplificación de trámites y mejora regulatoria, se considera que la afectación producto del ciberataque ha sido crítica, principalmente porque las actividades en buena medida, dependían de las tecnologías de información, por ejemplo, se disponía de un catálogo institucional de trámites expuesto en una Web institucional, con 38 gestiones con el objetivo de que fuera automatizado; asimismo, tenían la oportunidad de que el 100 % de los trámites fuera presencial, sin embargo, la oficina a cargo del proceso correspondiente depende totalmente de la plataforma tecnológica, por lo que el resultado de la afectación es general. Según lo manifestado por el Lic. Chacón Marín, actualmente se está aplicando una encuesta en las diferentes unidades para determinar el grado de afectación en trámites y si se dispone de algún plan de contingencia.

4. Consideraciones Finales

Es criterio de esta Auditoría que lo descrito en este oficio, llama a la reflexión de la administración activa, particularmente en cuanto a la importancia de promover una cultura de administración de gestión del riesgo. En adición, y de acuerdo con esa misma norma, el propósito de la gestión de riesgos es la creación y protección del valor, y a través de este proceso, mejorar el desempeño, fomentar la innovación y contribuir al logro de los objetivos. Es por ello, que no se debe perder de vista los principios de una gestión de riesgos, entendidos de la siguiente forma:

- Que estén integrados en todas las actividades de la organización.
- Que estén estructurados y sean exhaustivos, lo cual contribuye a que los resultados sean coherentes y comparables.
- Que el marco de referencia utilizado se adapte a lo interno y externo de la organización en función de sus objetivos.
- Que tenga la participación de todas las partes interesadas.
- Que sea dinámico, ya que los riesgos tienen a aparecer, desaparecer o cambiar, y la administración de riesgos, anticipa, detecta, reconoce y responde a esos cambios.
- Que la información sea oportuna, clara y disponible para las partes interesadas pertinentes.
- Que se consideren los factores humanos y culturales, como parte esencial del del desarrollo del pensamiento basado en riesgos.
- Que exista una mejora continua, mediante el aprendizaje y la experiencia de los eventos materializados.

Las Mejores Prácticas de Buen Gobierno Corporativo parten de un enfoque de Gestión del Riesgo y, dentro de él, la principal obligación del jerarca y la alta gerencia es mantener un apropiado Sistema de Gestión Integral, partiendo de la estrategia institucional que tenga en cuenta los riesgos de la organización, su impacto, mitigación y costo del control. Naturalmente, corresponderá a la administración su implementación y, a la alta gerencia, su evaluación posterior.

En tal sentido, se aportan los elementos analizados en este contexto, a fin de que sirvan de instrumento para la valoración y el monitoreo de riesgos que realizan esas gerencias y, de este modo, asesorar y contribuir en la toma de decisiones que correspondan a esos niveles jerárquicos, para garantizar, de forma oportuna y eficiente, la implementación de acciones para el mejoramiento del control interno, la administración de riesgos estratégicos y el fortalecimiento de los procesos de dirección relacionados con fortalecer la cultura de gestión de riesgos a nivel institucional.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.12 08:45:44 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/ANP/MZS/GAP/PAA/ghc

C. Dr. Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva - 1102
Auditoría