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

AS-AATIC-185-2022
6 de septiembre de 2022

Doctor
Álvaro Ramos Chaves, presidente ejecutivo
PRESIDENCIA EJECUTIVA - 1102

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
Gilberth Alfaro Morales, gerente a.i
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

Ingeniera
Susan Peraza Solano, directora
DIRECCIÓN DE PLANIFICACIÓN INSTITUCIONAL-2902

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

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150
CONSEJO TECNOLÓGICO INSTITUCIONAL

Estimados(as) señores(as):

ASUNTO:	**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.**

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, específicamente en su rol de asesor, esta Auditoría informa sobre la importancia de fortalecer los mecanismos de seguridad de la información y ciberseguridad en la CCSS, producto de los riesgos detectados mediante instrumento elaborado por la Contraloría General de la República como parte de la evaluación denominada: "Aplicación de prácticas de seguridad de la información en las instituciones públicas", en atención del oficio N°12680 (DFOE-CAP-2262). Lo anterior con el objetivo de que ese Consejo Tecnológico Institucional tenga conocimiento y adopte las medidas correspondientes acorde a su ámbito de acción y de acuerdo con las funciones establecidas en el Manual Funcional del Consejo Tecnológico de la CCSS.

Al respecto, el 1 de agosto de 2022, mediante oficio DFOE-CAP-2262, la Contraloría General de la República informó a los jerarcas de las Instituciones, Ministerios, Gobiernos Central y Locales, y empresas del Estado, que dicho Órgano actualmente desarrolla un proyecto de fiscalización posterior, de tipo Seguimiento de la gestión pública denominado: "Aplicación de prácticas de seguridad de la información en las instituciones públicas", el cual tiene como propósito determinar la aplicación de prácticas de seguridad de la información en las instituciones públicas, con base en el marco regulatorio y prácticas aplicables, con el fin de generar insumos para la toma de decisiones que permitan a la Administración promover mejoras en dicha gestión. Por lo anterior adjuntaron un archivo en el cual solicitaban fuera completado con la información correspondiente, y adjuntar el respaldo documental de las respuestas brindadas, dicho instrumento contenía consultas relacionadas con la gestión institucional en materia de Seguridad de la Información y Ciberseguridad.

Por lo anterior, se respondió el citado instrumento, mediante el oficio GF-DSCR-0424-2022 de fecha 22 de agosto de 2022 suscrito por el Lic. Luis Rivera Cordero, director de la Dirección del SICERE, quién obtuvo colaboración de diferentes funcionarios de la institución para el correspondiente llenado de la herramienta, y el mismo fue enviado a esta Auditoría el 23 de agosto de 2022 mediante el oficio PE-2148-2022 suscrito por el Dr. Álvaro Ramos Chaves, presidente ejecutivo. Al respecto, una vez analizada la información por parte de este Órgano de Fiscalización, se identificaron aspectos por atender que generan la probabilidad de materialización de riesgos en materia de seguridad de la información y ciberseguridad, mismos que se exponen a continuación:

- La Institución carece actualmente de un Sistema de Gestión de la Seguridad de la información (SGSI) que gestione eficientemente la accesibilidad de la información, asegure la confidencialidad, integridad y disponibilidad de los activos de información y que esté debidamente alineada con la estrategia institucional de Tecnologías de Información.

- No se disponen de procedimiento y/o políticas debidamente formalizadas en cuanto a clasificación de activos tecnológicos, e información según confidencialidad, integridad y disponibilidad, mecanismos sancionatorios ante incumplimiento de procedimientos y políticas.

- No existe la persona encargada del rol de oficial de seguridad de la información (CISO), ni la definición de un comité de seguridad de la información.

- No se ha formalizado un Plan de Contingencia basado en análisis de impacto al negocio, tampoco planes de recuperación de incidentes que incluya estrategias para minimizar los efectos de un desastre y permitir que se continúe con la operación normal de la organización o se reanude rápidamente las operaciones importantes, asimismo los sitios alternos de procesamiento de acuerdo con el análisis de impacto del negocio.

- No se establecen ni implementan mecanismos para la identificación de desviaciones conforme a la tolerancia-límite de riesgo definido como aceptable.

- La institución carece de estudios de impacto sobre el funcionamiento de la entidad en caso de materializarse riesgos relacionados con la pérdida de activos de información.

- Ante la ausencia de un Sistema de Gestión de la Seguridad de la Información, no se disponen de auditorías interna y/o externas que midan la eficacia de dicho sistema.

- No se aplican los protocolos y el marco normativo establecido por la entidad rectora en seguridad de la información y ciberseguridad (MICITT).

- La Institución no ha integrado la seguridad de la información a los distintos procesos institucionales, por cuanto se llevan como un proceso separado de la gestión operativa institucional.

- Se carece de mecanismos hacia el personal institucional como charlas, cursos, foros, evaluaciones y pruebas donde se evalúe su percepción y conciencia en materia de ciberseguridad.

- La Institución no dispone de un programa de concientización hacia el personal sobre la seguridad de la información, que considere aspectos como: los controles para proteger la información, funciones del personal y la promoción de conciencia sobre el riesgo de no seguir los procedimientos y/o políticas, campañas de concientización como publicación de folletos o boletines, actualización periódica considerando lecciones aprendidas de los incidentes de seguridad de la información y divulgación de los procedimientos disponibles para reportar violaciones de seguridad de la información.

- No se disponen de certificaciones relacionadas con el Sistema de Gestión de Seguridad de la Información ante la ausencia de este.

- Se han identificado y clasificado menos del 50% de la información crítica y/o sensible de la Institución.

- Si bien se ha elaborado el inventario de más del 50% de los activos y dispositivos informáticos, no se categorizan los activos que son identificados como críticos.

- Se omite realizar copias de los respaldos de la información en sitios alternos como centros de datos o en la nube, con el fin de que se pueda recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.

- No se encripta la información almacenada que es catalogada como crítica o sensible.

- No se disponen de mecanismos para encriptar la información en tránsito de aquella que es catalogada como crítica o sensible.

- Se carece de un EDR (Endpoint Detection and Response) que proporcione monitorización y análisis continuo del endpoint y la red, donde se identifique, detecte y prevenga amenazas con mayor facilidad.

- En cuando a la implementación de un plan para la gestión de incidentes, este carece de mecanismos alternos de adaptación donde el personal deba utilizarlo ante la ocurrencia de un incidente, no se dispone de tiempos de recuperación, pruebas de recuperación, definición de límites de pérdidas máximas de información después de la aplicación de planes de respuesta, afinamiento del proceso de recuperación, y la incorporación de lecciones aprendidas.

- No se han efectuado simulacros o pruebas de manejos de incidentes durante los años 2021 y 2022.

- La Institución no dispone de indicadores que midan el grado de seguridad alcanzado con las medidas ejecutadas a partir de los resultados de simulacros o pruebas de incidentes.

- No se dispone de un plan de capacitación en materia de Ciberseguridad.

Como se observa, son 22 debilidades las que se identifican en las respuestas dadas en el instrumento solicitado por el Órgano Contralor, de las cuales en su mayoría han sido expuestas por esta Auditoría en diversos productos, tal y como se señaló en el oficio de advertencia AD-AATIC-067-2022 el 31 de mayo de 2022 dirigido al Dr. Roberto Cervantes Barrantes, Gerente General, al Máster Roberto Blanco Topping, Subgerente a.i. y la Máster Mayra Ulate Rodríguez, jefe del Área de Seguridad y Calidad Informática, ambos de la Dirección de Tecnologías de Información y Comunicaciones, donde se informa que si bien la Institución ha formulado acciones relacionadas al tema, esta Auditoría ha sido insistente en diferentes momentos para señalar a la Administración oportunidades de mejora relacionadas con la disponibilidad de estrategias avanzadas de ciberseguridad, previo a la materialización del riesgo y recientemente dando énfasis a las consideraciones pertinentes bajo el contexto actual, enlistando 37 productos emitidos al respecto **(ver anexo)**.

Al respecto 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 XI, Seguridad y Ciberseguridad, lo siguiente:

> *"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.*
>
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.*
>
> *La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*
>
> *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.*
>
> *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales".*

El Manual Funcional del Consejo Tecnológico de la CCSS en el punto 8.2 "Funciones sustantivas del Consejo Tecnológico" establece:

> *"**8.2.1 Estrategia***
>
> *1) Velar por la alineación de la estrategia tecnológica con la estrategia institucional, de forma que las acciones desarrolladas por la DTIC y otras instancias institucionales se orienten al logro de esas estrategias. (…)*

5) Valorar y aprobar las estrategias de asignaciones internas y externas, que permitan el máximo aprovechamiento de los recursos financieros, humanos y tecnológicos que soportan las TIC de la CCSS. (…)

7) Validar los procesos de gobernanza TIC, así como sus modificaciones periódicas. (…)

10) Valorar Plan de Recursos y Estrategias de aprovisionamiento TIC, verificando la alineación con la planificación financiera institucional y de Recursos Humanos y realizando las observaciones y recomendaciones que se consideren necesarias, de acuerdo con el proceso EDM04 - Asegurar la optimización de recursos.

8.2.2 Control y seguimiento

1) Revisar la medición del desempeño y la contribución de TI con el negocio, conforme lo establecido en los procesos de monitoreo de gobernanza TIC: EDM01 "Asegurar el establecimiento y mantenimiento del marco de gobernanza", proceso institucional de Banco de Iniciativas y Portafolio Institucional de Proyectos (específicamente en lo que se refiere a proyectos con componente TIC), EDM04 "Asegurar la gestión de los recursos de TIC", EDM05 "Asegurar la transparencia hacia las partes interesadas".

2) Dar seguimiento periódico a los riesgos críticos de TI y los planes de respuesta que se están implementando.

8.2.3 Normativa TIC

1) Validar la definición o modificación de Políticas y Reglamentos que norman la gobernanza TIC a nivel institucional, de acuerdo con las responsabilidades de revisión y aprobación designadas en Lineamientos para la generación y administración de normativa y documentación TIC.

8.2.4 Valor y beneficios TIC

1) Dar seguimiento a proyectos estratégicos TIC o con componente TIC, con el fin 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.

2) Aprobar los mecanismos para el control y monitoreo del rendimiento y logro de los beneficios de las inversiones de negocio en proyectos con componentes TIC".

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de ser sometidas a valoración y revisión por ese Consejo Tecnológico, se adopten las medidas pertinentes y así coadyuvar a la mitigación de las vulnerabilidades identificadas, cumpliendo con los objetivos institucionales, así como de la normativa legal y técnica especialmente la que involucra el tema tratado en el presente oficio, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad Informática.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.09.06 16:37:18 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

Anexo (1)

1. Oficio AD-AATIC-067-2022.

C. Auditoría