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

Al contestar refiérase a: **ID-121219**
CONFIDENCIAL

AD-ATIC-0085-2024
12 de agosto de 2024

Máster
Marta Eugenia Esquivel Rodríguez, presidente en calidad de coordinadora
Consejo Tecnológico
PRESIDENCIA EJECUTIVA - 1102

Máster
Robert Picado Mora, subgerente en calidad de secretario
Consejo Tecnológico
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimado (a) señor (a):

ASUNTO: Oficio de Advertencia referente a la gestión de Seguridad de la Información y Ciberseguridad en la CCSS de acuerdo con los estándares ISO 27001 y NIST.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2024 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 los resultados del proyecto de Auditoría denominado “Auditoría de Carácter Especial referente a la gestión de Seguridad de la Información y Ciberseguridad en la CCSS de acuerdo con los estándares ISO 27001 y NIST”, mismo que se trabajó en colaboración con la Contraloría General de la República, donde a través de reuniones así como mediante el oficio DFOE-IAF-0010 del 29 de febrero de 2024, suscrito por la Licda. Jessica Víquez Alvarado, gerente de área de la División de Fiscalización Operativa y Evaluativa, se suministraron herramientas relacionadas con la gestión de la Seguridad de la Información y Ciberseguridad mediante el estándar ISO 27001 y el marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), con el propósito de analizar si los procesos de gestión de seguridad de la información y ciberseguridad de la Institución, están razonablemente alineados con el marco jurídico y técnico relacionados en esta materia. Lo anterior con el objetivo de informar sobre los resultados obtenidos y que se adopten las medidas correspondientes acorde a su ámbito de acción.

En virtud de lo anterior y una vez ejecutado los procedimientos correspondientes, en conjunto con la información suministrada por funcionarios adscritos a las diferentes Gerencias de la Institución se detalla a continuación los resultados:

1. GENERALIDADES

1.1. Antecedentes

Actualmente, la información se ha convertido en uno de los activos más valiosos para las organizaciones e Instituciones. La protección de estos datos es esencial para mantener la confidencialidad, integridad y disponibilidad de la información, evitando pérdidas financieras, daños reputacionales y compromisos legales. La seguridad de la información y la ciberseguridad, que se centran en proteger los sistemas, redes y datos de ataques, daños y acceso no autorizado, son fundamentales para la operación segura y eficiente de los procesos organizacionales.

Una gestión adecuada de la seguridad de la información implica no solo la implementación de tecnologías y herramientas avanzadas, sino también la adopción de políticas, procedimientos y controles que aseguren un enfoque integral y sistemático para la protección de los activos de información, donde sean los responsables del Negocio, quienes asuman estas actividades al ser los administradores e incluso dueños de los datos gestionados. Normas como la ISO 27001 y los estándares del NIST proporcionan marcos estructurados para la gestión de la seguridad de la información, ayudando a las organizaciones a identificar riesgos, implementar controles adecuados y mantener la seguridad en el tiempo y así mitigar riesgos.

A nivel de la CCSS, si bien se han formulado acciones relacionados con la Seguridad de la Información y la Ciberseguridad, las mismas se han centrado principalmente en esta segunda; omitiendo el abordaje de los riesgos relacionados con la protección de datos que no necesariamente están automatizados o bien con el uso que se le da a la información en los procesos institucionales.

Al respecto, posterior al ciberataque sufrido en la CCSS el 31 de mayo del 2022, la Dirección de Tecnologías de Información y Comunicaciones con el apoyo de diversos proveedores como Deloitte, Microsoft, GBM, así como entes asesores, tales como: el Centro Criptológico Nacional Español (CN-CERT), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y productos emitidos por la Auditoría Interna, identificó una serie de lecciones aprendidas y procesos de mejora que debían ser incorporados en los esfuerzos que la Institución venía realizando, específicamente al “Plan de Ciberseguridad” que se aprobó en el 2020.

Por lo anterior, la DTIC elaboró una actualización del Programa denominado: “Fortalecimiento del Plan de Ciberseguridad”, el cual contempló las necesidades originales, así como otras recomendaciones que fueron detectadas a raíz del ataque cibernético sufrido, con el objetivo de robustecer el marco de ciberseguridad institucional y minimizar los riesgos para que una situación como la acontecida tenga el menor impacto posible en la prestación de los servicios que brinda la CCSS.

Mediante oficio GG-DTIC-6654-2022 del 18 de noviembre de 2022, este programa se remitió a la Gerencia General, bajo el nombre “Plan de Fortalecimiento Proyecto Ciberseguridad”, cuyo objetivo era presentar una propuesta de abordaje que cubriera todas las necesidades originales, así como otras recomendaciones a raíz del ataque cibernético sufrido en la Caja Costarricense del Seguro Social el 31 de mayo de 2022 por parte de entes externos a la Institución.

La estrategia planteada constituyó un compendio de iniciativas propuestas en un marco de abordaje integral, que permitiera en su conjunto atender una serie de acciones requeridas para reforzar la seguridad cibernética. Este conjunto de iniciativas correspondía a 34 propuestas, de las cuales 28 respondía a acciones de ciberseguridad, en tanto 6 a seguridad de la información, el mismo fue presentado al Consejo Tecnológico el 23 de enero de 2023 por parte del Ing. Danilo Hernández Monge, antes subdirector de la DTIC, y la Ing. Ericka Sánchez Solís, analista en sistemas de la DTIC, no obstante en esa oportunidad en los acuerdos tomados por el Consejo Tecnológico no se dio una aprobación formal del Plan reforzado.

Posteriormente, y después de una revisión efectuada por el Área de Seguridad y Calidad Informática, el 21 de junio del 2024, se presentó ante el Consejo Tecnológico, la propuesta de la hoja de ruta del Programa de Ciberseguridad, misma que fue aprobada y tuvo como resultado el traslado a la función operativa de la DTIC de 8 iniciativas, 4 iniciativas fusionadas en dos, 17 iniciativas a ejecutarse del II semestre de 2024 a al I semestre de 2027 y 7 iniciativas relacionadas con la seguridad de la información, donde en dicha hoja de ruta se señala al respecto:

"En este caso particularmente, el Área de Seguridad y Calidad Informática tiene un rol de acompañamiento y asesoría, no obstante, la seguridad de la Información contempla un enfoque de negocio, por lo cual, en el marco de la Gobernanza de las TIC, es desde la administración activa de la institución que se debe liderar y ejecutar lo correspondiente para su aplicación.

Por lo anterior, una vez analizadas las iniciativas se describen las que están relacionas con la seguridad de la información para lo cual necesitamos el apoyo del negocio en el cual el Área de Seguridad y Calidad Informática sería un ente asesor para el desarrollo de estas (…)"

En línea con lo anterior, la Auditoría Interna de la CCSS en colaboración de la Contraloría General de la República, con el objetivo de verificar si los procesos de gestión de seguridad de la información y ciberseguridad de la Institución están razonablemente alineados con el marco jurídico y técnico, comunicó el 13 de marzo de 2024, mediante oficio AI-0453-2024, a la Máster Marta Eugenia Esquivel Rodríguez, presidenta Ejecutiva, a la Máster Vilma Campos, gerente General a.i. y al Ing. Robert Picado Mora, subgerente de la DTIC, el inicio del presente estudio, trasladando posteriormente el 19 de abril de 2024, mediante oficio AI-0613-2024 dirigido al Ing. Daniel Berrocal Zúñiga, jefe a.i. del Área de Seguridad y Calidad Informática, dos instrumentos de verificación relacionados con el estándar ISO 27001 y el marco de Ciberseguridad NIST para su respectivo llenado.

Posterior al análisis realizado por parte del Ing. Berrocal con su equipo de trabajo, se concluyó que se requería del apoyo de los responsables del negocio para el llenado de las herramientas facilitadas por el Órgano Contralor, por lo que el Máster Robert Picado Mora, mediante oficio GG-DTIC-3046-2024 del 13 de mayo de 2024, le solicitó a la Ing. María de los Ángeles Gutiérrez Brenes, gerente General a.i. y a la Licda. Gabriela Artavia Monge, gerente Administrativa a.i. la participación de un funcionario para integrar el equipo intergerencial para el llenado de los instrumentos en mención. Es así como el 17 de mayo de 2024, mediante el oficio GG-0678-2024, la Ing. Gutiérrez Brenes, solicitó a todo el cuerpo gerencial de la Institución, un representante para integrar el equipo correspondiente.

Por lo anterior, el 3 de julio de 2024, mediante oficio GG-DTIC-4270-2024, el Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática le remitió al Máster Robert Picado Mora, subgerente de la DTIC, los cuestionarios "01 - Herramienta GSI" y "02 - Checklist NIST CSF" debidamente completados por el equipo de trabajo designado, en coordinación con las distintas gerencias, el cual estuvo integrado por los siguientes funcionarios:

- Ing. Roy Ovares Valerio, CGI, Gerencia Logística
- Ing. Roger Muñoz Díaz, Asesor Despacho, Gerencia Administrativa
- Ing. Mario Villalobos Marín, CGI Gerencia Pensiones
- Ing. José Antonio Vargas Solís, CGI Gerencia Financiera
- Lic. Joseph Morales Porras, CGI Gerencia Infraestructura y Tecnologías
- Dr. Luis Enrique Sánchez Rodríguez, Despacho, Gerencia Médica
- Ing. Dennis Figueroa Quirós, CGI Gerencia Médica
- Ing. Ronald Guzmán Vásquez, informático del Área de Estadísticas en Salud, Gerencia
- Médica
- Ing. Erick Vindas Umaña, jefe Subárea Seguridad en Tecnologías de Información

- Máster Mario Vílchez Moreira, jefe, Subárea Aseguramiento de la Calidad en Tecnologías
- de Información

1.2. Estándares ISO 27001 y NIST

La norma ISO 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), ISO/IEC 27001 proporciona un marco de trabajo para ayudar a las organizaciones a proteger sus activos de información y gestionar los riesgos relacionados con la seguridad de la información de manera sistemática y efectiva.

Es una realidad actual que las organizaciones están expuestas a múltiples amenazas como lo son fallos energéticos, virus informáticos, fraude, error humano, fallo de elementos, accesos indebidos, desastres naturales, vandalismo, entre otros, a las que son vulnerables y para cuya gestión deben estar preparadas. La implementación de un sistema de gestión de seguridad de la información bajo los requisitos de la norma ISO 27001, permite minimizar la probabilidad de materialización de las amenazas y estar preparados para disminuir su impacto en caso de que se materialicen.

La norma ISO 27001 define 93 controles, los cuales se categorizan en 4 áreas en la Seguridad de la Información: organizativos, personal, seguridad física y tecnología. Además de la categorización en temas, se utilizan atributos que permiten crear diferentes vistas de los controles, las mismas ofrecen perspectivas variadas, que pueden adaptarse a diferentes necesidades. Los atributos se emplean para filtrar, ordenar y presentar los controles en formas específicas.

Cada control se asocia a cinco atributos, que son:

a) **Tipo de control:** Define si el control es preventivo, detectivo o correctivo, según su influencia en la ocurrencia y manejo de incidentes de seguridad.

b) **Propiedades de la seguridad de la información:** Indica si el control contribuye a la confidencialidad, integridad o disponibilidad de la información.

c) **Conceptos de ciberseguridad:** Relaciona el control con los conceptos de identificar, proteger, detectar, responder y recuperar de acuerdo con el marco de ciberseguridad.

d) **Capacidades operativas:** Muestra cómo el control impacta en áreas como gobernanza, gestión de activos, seguridad de sistemas, entre otras.

e) **Dominios de seguridad:** Clasifica el control en cuatro dominios de seguridad: gobernanza y ecosistema, protección, defensa y resiliencia.

Por su parte, el Marco de Ciberseguridad NIST, forma parte de una serie de documentos y pautas desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Estas

normas proporcionan un marco de referencia para ayudar a las organizaciones a gestionar y mejorar su postura de seguridad cibernética y proteger la información sensible.

El NIST Framework es una guía basada en estándares, pautas y prácticas existentes, en la cual una organización puede administrar y reducir el riesgo de ciberseguridad. Asimismo, permite fomentar la comunicación de gestión de riesgos y ciberseguridad entre todas las partes interesadas de la organización tanto internas como externas.

Este Marco incluye funciones, categorías, subcategorías y referencias informativas, tal y como se detalla:

- **Función:** Se organizan actividades básicas de seguridad cibernética en su nivel más alto. Estas funciones son Identificar, Proteger, Detectar, Responder y Recuperar.

- **Categoría:** Son las subdivisiones de una Función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares. Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".

- **Subcategorías:** Dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada Categoría.

- **Referencias informativas:** son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría.

1.3. Acciones implementadas por la CCSS en torno a la Seguridad de la Información

La Institución ha formulado y se encuentra en ejecución el Modelo de Gobernanza de las TIC y de Seguridad de la Información, el cual fue gestionado mediante a licitación abreviada No. 2016LA-000003-1150 “Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS”, que tuvo como fin, contratar una consultoría que apoyara la obtención de un modelo de gobernanza en tecnologías de información y en seguridad de la información.

Particularmente, el entregable de la Fase 4 “Analizar las brechas integrales del Gobierno de las Tecnologías de Información y Comunicaciones evaluando el Gobierno de la Seguridad de la Información”, diagnosticó el ambiente institucional en ese momento, donde en el apartado 5.5 “Análisis del Modelo de Gestión de Seguridad de la Información”, del Informe Diseño del modelo meta integral de gobernanza de la TIC y Seguridad de la Información, refiere sobre la visión estratégica, los siguientes hallazgos clave:

- No existen iniciativas institucionales impulsadas por la Alta Direccion que permitan consolidar un modelo de gestión de seguridad de la información.

- Existe un entendimiento asociado a la seguridad de la información que se centra únicamente en el aseguramiento de la soluciones y plataformas tecnológicas, caracterizado por la delegación de responsabilidad sobre la seguridad a las unidades de TIC, por lo que no existe el involucramiento y corresponsabilidad por parte de los usuarios.

En cuanto a gestión de seguridad de la información, los hallazgos señalados por la Consultora fueron:

- La gestión de la seguridad se enfoca en la protección de la infraestructura tecnológica y el acceso a las aplicaciones.
- No existe una identificación de los activos de información institucionales, por lo cual no se tiene una clasificación de éstos según su criticidad y sensibilidad.
- La gestión de la seguridad tiene un enfoque reactivo ya que no se conoce la visión estratégica institucional con respecto al nivel de protección que requieren los activos de información. Por otra parte, de acuerdo con lo indicado por la firma consultora, se hace necesario cubrir las brechas identificadas para lograr la implementación del modelo meta propuesto, planteando estructuras, tanto para la gobernanza, como para la gestión de la seguridad de la información.

En este sentido, se definieron cuatro iniciativas relacionadas con el Modelo de Seguridad de la Información, las cuales actualmente se encuentran en el siguiente estado:

Cuadro No. 1
Porcentaje de avance de las iniciativas relacionadas con el Modelo de Seguridad de la Información

Iniciativa	% de avance
Habilitar la gestión de operaciones de TIC desde la perspectiva de las seguridades operativas	95%
Establecer el Plan Táctico de Ciberseguridad	70%
Habilitación del Comité de Riesgos y Seguridad de la información	0%
Implementar el Sistema de Gestión de Seguridad de la Información	0%

Fuente: Informe ejecutivo de Programas y Proyectos Estratégicos para la Junta Directiva, I trimestre de 2024.

Como se observa las iniciativas de habilitación del Comité de Riesgos y Seguridad de la información e Implementar el Sistema de Gestión de Seguridad de la Información, no ha tenido un avance en su implementación, a pesar de que dicho Modelo fue diseñado en el 2017.

Asimismo, es conveniente mencionar la importancia de los roles y responsabilidades especializados en materia de seguridad de la información y ciberseguridad, los cuales fueron detallados anterioridad por la empresa consultora PWC en los entregables del proyecto de “Gobernanza TIC y Seguridad de la Información” y “Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS”, compilados en el siguiente cuadro:

Cuadro No. 2
Identificación de roles clave diseño de modelo de Gobernanza TIC y Seguridad de la Información (2017) y Plan de Ciberseguridad para la CCSS (2020)

Rol	Descripción breve de la Responsabilidad
Comité de Riesgos y Seguridad	Este comité es el encargado de garantizar el adecuado seguimiento y revisión de los mecanismos implantados dentro de la CCSS para el aseguramiento de la información, evaluando, proponiendo y discutiendo las estrategias y prácticas estándares aplicables en cada escenario. Se encuentra integrado por Representantes de Junta Directiva, Ejecutivo de Seguridad de la Información, Ejecutivo de Riesgo Institucional, Ejecutivo de Continuidad De Servicios, director Actuarial, Gestor de Seguridad Informática, Dueños de Servicios y Procesos Institucional Clave, Director de la Dirección de Tecnologías de Información y Comunicaciones.
Ejecutivo de Seguridad de la Información	Es la figura de negocio responsable de implementar y mantener una estrategia de seguridad de la información para la organización.
Ejecutivo de Riesgo Institucional	Es la figura de negocio responsable de apoyar en la definición Apetito de Riesgo de la Institución, direccionar a la Alta Gerencia sobre la toma de decisiones relacionada con la evaluación, los controles, la optimización, el monitoreo y el financiamiento de las estrategias de mitigación de los riesgos que debe afrontar la CCSS, permitiendo de esta manera generar declaraciones formales sobre los lineamientos que deben de cumplirse en los diferentes niveles de gobernabilidad y gestión de las operaciones internas que soporta la institución.
Ejecutivo de Continuidad de Servicios	Es la figura de negocio responsable de diseñar, gestionar, supervisar y evaluar las capacidades de continuidad de la Institución, con el fin de garantizar que la continuidad de los procesos de la institución antes situaciones de adversidad.
Director Actuarial	Es la figura de negocio responsable de apoyar la gestión de riesgos institucional en el análisis, evaluación y proyección de información económica y financiera.
Dueños de Servicios y Procesos Institucionales	Este rol posee un perfil de Dirección Institucional. En otras organizaciones llamados también “Dueños de Negocio”, los Dueños del Servicio Institucional son aquellas figuras dentro de la CCSS que poseen amplio conocimiento de los servicios brindados por la Institución y los procesos internos (ya sean operativos o automatizados) que apoyan estos servicios.
Gestor de Seguridad Informática	Este rol posee un perfil de Tecnologías de la Información. Es la figura responsable de la gestión, diseño, supervisión y evaluación la seguridad de la información bajo el enfoque de la seguridad informática.
Usuarios de la Información	Figura o ente interno o externo a la Institución que hace uso de la información o es un potencial consumidor o generador de la misma.
Gestor de ciberseguridad	Garantiza la aplicación de la normativa interna y externa relacionada con la Seguridad de la Información en los procesos y servicios TIC, así como, establecer estrategia de ciberseguridad que apoyen en el cumplimiento regulatorio.
Arquitecto de ciberseguridad	Establece criterios, marcos de referencia, estándares y orientación experta sobre la arquitectura tecnológica de ciberseguridad, en términos de su operación, estandarización y evolución de cara a la visión de arquitectura empresarial de la CCSS y en alineamiento con el Sistema de Seguridad de la Información institucional.
Técnico de monitoreo.	Monitorea los servicios TIC e infraestructura tecnológica a fin de gestionar eventos e incidentes que afecten la disponibilidad, capacidad y ciberseguridad.
Roles TIC con responsabilidades de ciberseguridad	Integrar la ciberseguridad a las diferentes áreas que proveen los servicios TIC.

Fuente: Elaboración propia, a partir de entregables del proyecto de “Gobernanza TIC y Seguridad de la Información” y “Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS”.

2. RESULTADOS DE LA APLICACIÓN DE LOS INSTRUMENTOS ISO 27001 Y NIST

2.1 HERRAMIENTA GSI ESTÁNDAR ISO 27001

Se efectuaron 127 consultas a la administración activa, cuyas respuestas tenían como criterio de cumplimiento los siguientes:

Cumplimiento	Puntaje	Criterio
No	0	Falta cualquier elemento básico. Estrategia incompleta para abordar el propósito El proceso puede haberse definido o no
Parcial	5	Logra más o menos su propósito Actividades completas básicas No están estandarizadas
Si	10	Se logra el propósito Las actvidades estan definidas Se definieron estándares

Con base a las respuestas brindadas y verificadas por esta Auditoría, los criterios de resultados se midieron de la siguiente forma:

Resultado			Razonabilidad
85%	-	100%	Es satisfactorio
70%	-	85%	Tiene oportunidad de mejora
0%	-	70%	Requiere acciones inmediatas de mejora

Tipo de Control

En cuanto a los controles por tipo (preventivo, detectivo o correctivo), la Institución requiere de acciones inmediatas de mejora en los controles correctivos, y oportunidad de mejora en los preventivos y detectivos, como se observa:

Tipo de control	Número de preguntas	Si	No	Parcial	%	Evaluación individual
Preventivo	109	52	4	53	72%	Tiene oportunidad de mejora
Detectivo	14	6	0	8	71%	Tiene oportunidad de mejora
Correctivo	16	6	0	10	69%	Requiere acciones inmediatas de mejora

Al respecto, los controles correctivos están diseñados para mitigar los efectos de incidentes de seguridad una vez que ocurren y restaurar la operación normal, lo que implica que la Institución puede estar expuesta a riesgos prolongados o no recuperarse adecuadamente de incidentes.

Clasificación de Controles

Sobre la Clasificación de Controles, la Institución requiere de acciones inmediatas de mejora en 3 de los 4 los controles (organizativos, personas y físicos) y oportunidad de mejora en los controles tecnológicos, como se observa:

Clasificación de controles	Número de preguntas	Si	No	Parcial	%	Evaluación individual
Controles organizativos	50	16	1	33	65%	Requiere acciones inmediatas de mejora
Controles personas	9	3	0	6	67%	Requiere acciones inmediatas de mejora
Controles físicos	17	5	0	12	65%	Requiere acciones inmediatas de mejora
Controles tecnológicos	47	32	3	12	81%	Tiene oportunidad de mejora

Respecto a lo anterior, los controles organizativos establecen las políticas, procedimientos y estructuras necesarias para gestionar la seguridad de la información de manera efectiva, lo que pone en riesgo la seguridad general de la Institución. Los controles de personas se centran en las prácticas y comportamientos de los funcionarios que afectan la seguridad de la información, por lo que ante deficiencias críticas en estos controles, se pueden generar errores humanos y fallos de seguridad, asimismo, los controles físicos protegen los activos de información contra accesos no autorizados y daños físicos, exponiendo los activos de información a riesgos físicos.

Dominios de Seguridad

En cuanto a los dominios de seguridad, la Caja tiene oportunidades de mejora en los dominios de identificar, proteger, detectar y recuperar, y requiere de atención inmediata de mejora el dominio de responder, como se detalla:

Dominios de ciberseguridad	Número de preguntas	Si	No	Parcial	%	Evaluación individual
Identificar	30	13	1	16	70%	Tiene oportunidad de mejora
Proteger	92	44	3	45	72%	Tiene oportunidad de mejora
Detectar	17	7	0	10	71%	Tiene oportunidad de mejora
Responder	13	4	0	9	65%	Requiere acciones inmediatas de mejora
Recuperar	6	3	0	3	75%	Tiene oportunidad de mejora

Al respecto, el dominio de Responder abarca las capacidades y procesos necesarios para reaccionar adecuadamente ante incidentes de seguridad, por lo que pone en riesgo la capacidad de la Institución para manejar y mitigar incidentes de manera efectiva.

Capacidades operativas

Sobre las capacidades operativas, se identificó que la Caja de 15 de ellas, en 9 se requieren acciones de atención inmediatas de mejora, siendo Continuidad y Gestión de amenazas y vulnerabilidades, las de mayor atención con un puntaje de 50%, en 3 se tiene oportunidad de mejora y 3 se consideran satisfactorias como se observa:

Capacidades operativas	Número de preguntas	Si	No	Parcial	%	Evaluación individual
Aseguramiento de la seguridad de la información	5	2	0	3	70%	Tiene oportunidad de mejora
Configuración segura	10	4	2	4	60%	Requiere acciones inmediatas de mejora
Continuidad	7	1	1	5	50%	Requiere acciones inmediatas de mejora
Gestión de amenazas y vulnerabilidades	2	0	0	2	50%	Requiere acciones inmediatas de mejora
Gestión de eventos de seguridad de la información	15	4	0	11	63%	Requiere acciones inmediatas de mejora
Gestión de la identidad y del acceso	13	8	0	5	81%	Tiene oportunidad de mejora
Gestión de activos	23	5	1	17	59%	Requiere acciones inmediatas de mejora
Gobernanza	10	3	1	6	60%	Requiere acciones inmediatas de mejora
Legal y cumplimiento	8	3	0	5	69%	Requiere acciones inmediatas de mejora
Protección de la información	19	7	0	12	68%	Requiere acciones inmediatas de mejora
Seguridad de las aplicaciones	21	18	0	3	93%	Es satisfactorio
Seguridad de las relaciones con los proveedores	7	6	0	1	93%	Es satisfactorio
Seguridad de los recursos humanos	6	3	0	3	75%	Tiene oportunidad de mejora
Seguridad de los sistemas y de las redes	23	20	0	3	93%	Es satisfactorio
Seguridad física	19	5	0	14	63%	Requiere acciones inmediatas de mejora

Al respecto, considerando las capacidades operativas que requieren acciones inmediatas de mejora, se tiene que:

- La configuración de sistemas no está completamente asegurada, lo que puede llevar a vulnerabilidades explotables.
- Los planes de continuidad del negocio y recuperación ante desastres podrían no ser adecuados para asegurar la resiliencia operativa.
- Falta un proceso robusto para identificar, evaluar y mitigar amenazas y vulnerabilidades.
- La Institución carece de una respuesta efectiva y coordinada ante incidentes de seguridad de la información.
- La identificación y gestión de activos de información no es completa ni precisa.
- Falta una estructura clara de gobernanza para la gestión de la seguridad de la información.
- Los controles legales y de cumplimiento no están completamente implementados o actualizados.
- Las medidas de protección de información no son suficientes para proteger contra accesos no autorizados y pérdidas de datos.
- Las instalaciones físicas no están adecuadamente protegidas contra accesos no autorizados y desastres naturales.

2.1 HERRAMIENTA CHECK LIST NIST CSF

Se efectuaron 108 preguntas a la administración activa, para evaluar el nivel en que la Institución se encuentra, de acuerdo con los mínimos establecidos en el marco NIST. Para este caso, las respuestas tenían como criterio de valoración el nivel en que está la Institución del 1 al 4, donde para cada uno de ellos tiene la siguiente descripción:

Nivel		Criterio General
1	Parcial	Falta cualquier elemento básico. Estrategia incompleta para abordar el propósito El proceso puede haberse definido o no
2	Riesgo informado	Logra más o menos su propósito Actividades completas básicas No están estandarizadas
3	Repetible	Se logra el propósito Las actividades están definidas Se definieron estándares
4	Adaptado	Se logra su propósito, está bien definido. Su rendimiento se mide para mejorar el desempeño Se persigue la mejora continua

Resultados por Función

A nivel general, considerando los datos por función, la Institución registra la siguiente calificación de acuerdo con la valoración dada a cada una de las 108 preguntas:

Total por función	Calificación
IDENTIFICAR (ID)	75%
PROTEGER (PR)	76%
DETECTAR (DE)	79%
RESPONDER (RS)	92%
RECUPERAR (RC)	56%

De los resultados anteriores se puede indicar por cada función que:

- **La función Identificar** muestra que la Institución tiene una comprensión de sus activos, riesgos, políticas y procedimientos relacionados con la ciberseguridad, sin embargo, hay margen para mejorar en la gestión y la evaluación continua de estos aspectos.

- **La función Proteger** indica que la Institución tiene controles de seguridad establecidos para salvaguardar sus sistemas y datos, sin embargo, estos controles pueden mejorarse para ofrecer una mayor protección contra las amenazas.
- **La función Detectar** muestra que la Institución tiene capacidades de monitoreo y detección adecuadas para identificar incidentes de seguridad, sin embargo, hay oportunidades para mejorar la eficiencia y efectividad de estos procesos.
- **La función Responder** refleja una fuerte capacidad de respuesta ante incidentes de seguridad. La Institución está preparada para manejar y mitigar incidentes de manera efectiva.
- **La función Recuperar** indica que hay deficiencias significativas en la capacidad de la Institución para restaurar servicios y operaciones normales después de un incidente de seguridad, siendo este el área que requiere más atención y mejoras inmediatas.

Resultados por Categoría

Al analizar los resultados por función y categoría, se obtuvo lo siguiente:

Función	Categoría	Calificación
IDENTIFICAR (ID)	Asset Management (ID.AM): Gestión de activos	79%
	Business Environment (ID.BE): Entorno Empresarial	75%
	Governance (ID.GV): Gobernanza	69%
	Risk Assessment (ID.RA): Evaluación de riesgos	88%
	Risk Management Strategy (ID.RM): Estrategia de gestión de riesgos	67%
	Supply Chain Risk Management (ID.SC): Gestión del riesgo de la cadena de suministro	75%

Del cuadro anterior, se observa que la categoría **gobernanza** se encuentra en un nivel moderado, indicando que hay políticas, procedimientos y procesos de seguridad de la información establecidos, pero existe un margen de mejora, asimismo, **la estrategia de gestión de riesgos** muestra áreas significativas para mejorar, especialmente en la formalización y comunicación de estrategias de gestión de riesgos.

Función	Categoría	Calificación
PROTEGER (PR)	Identity Management, Authentication and Access Control (PR.AC): Gestión de identidad, autenticación y control de acceso	79%
	Awareness and Training (PR.AT): Concienciación y capacitación	75%
	Data Security (PR.DS): Seguridad de los datos	75%
	Information Protection Processes and Procedures (PR.IP): Procesos y procedimientos de protección de la información	75%
	Maintenance (PR.MA): Mantenimiento	75%
	Protective Technology (PR.PT): Tecnología de protección	60%

Respecto a las Categorías de la Función Proteger, como se observa, **la protección de la tecnología** es el área más débil dentro de esta, lo que indica que los sistemas tecnológicos y las soluciones de seguridad no están adecuadamente protegidos contra amenazas.

Función	Categoría	Calificación
DETECTAR (DE)	Anomalies and Events (DE.AE): Anomalías y eventos	80%
	Security Continuous Monitoring (DE.CM): Monitoreo continuo de la seguridad	78%
	Detection Processes (DE.DP): Procesos de detección	80%

Sobre las Categorías de la Función Detectar, se observa una gestión de seguridad razonablemente sólida en cuanto a la detección de anomalías y eventos, el monitoreo continuo y los procesos de detección, sin que esto no signifique que se pueda seguir mejorando y fortaleciendo aún más estas capacidades.

Función	Categoría	Calificación
RESPONDER (RS)	Response Planning (RS.RP): Planificación de la respuesta	100%
	Communications (RS.CO): Comunicación	100%
	Analysis (RS.AN): Análisis	100%
	Mitigation (RS.MI): Mitigación	83%
	Improvements (RS.IM): Mejoras	75%

En cuanto a la Función Responder, las Categorías de esta determina que la Institución tiene una buena capacidad en la planificación de la respuesta, comunicaciones y análisis de incidentes, y las áreas de mitigación y mejora continua, presentan un margen para optimizar aún más estas categorías.

Función	Categoría	Calificación
RECUPERAR (RC)	Recovery Planning (RC.RP): Planificación de la recuperación	50%
	Improvements (RC.IM): Mejoras	50%
	Communications (RC.CO): Comunicaciones	67%

Como se mencionó anteriormente, la función Recuperar indica que hay deficiencias significativas en la capacidad de la Institución para restaurar servicios y operaciones normales después de un incidente de seguridad, por lo que es esta la que debe recibir mayor atención debido a los bajos porcentajes de sus categorías, en las que se señala que:

- **La planificación de la recuperación** está en un nivel bajo, lo que sugiere que la Institución necesita mejorar significativamente sus planes de recuperación para asegurar una restauración rápida y eficiente de las operaciones tras un incidente.

- **La capacidad de mejorar** continuamente los procesos de recuperación es baja, lo que indica que la Institución necesita establecer un ciclo de retroalimentación más efectivo para aprender de los incidentes y mejorar sus capacidades de recuperación.

- **Las comunicaciones** durante y después de un proceso de recuperación están en un nivel moderado, indicando que, aunque hay una base establecida, existe margen de mejora para asegurar una comunicación más efectiva con todas las partes interesadas.

3. CONSIDERACIONES NORMATIVAS

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado IX. “Seguridad y Ciberseguridad”, menciona 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."

Las Normas de Control Interno para el sector público, en el punto 4.1 "Actividades de Control", señala:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad. (…)"

Asimismo, en el punto 4.4 "Exigencia de Confiabilidad y oportunidad de la información" indica:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas"

En el punto 5.6 "Calidad de la Información" de la misma norma se señala:

"El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo".

Además, en el punto 5.8 "Control de Sistemas de Información", establece:

"El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter".

Y finalmente en el punto 5.9 "Tecnologías de Información", indica:

"El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información (…)".

4. CONSIDERACIONES FINALES

La importancia para la CCSS de tener un adecuado control de la seguridad de la información y la ciberseguridad no puede subestimarse en el entorno digital actual. Con el aumento de las amenazas cibernéticas, es esencial que la Institución adopte medidas proactivas y efectivas para proteger sus datos y sistemas de información, como unos de los principales activos que tiene la CCSS debido a la transformación digital que han tenido los diferentes procesos sustantivos Institucionales y donde especialmente se gestiona información de la población, es por esto que el uso de estándares reconocidos internacionalmente, como la ISO 27001 y el marco de Ciberseguridad NIST, proporciona una base sólida para el desarrollo de políticas y procedimientos de seguridad robustos.

En cuanto a los resultados de la evaluación de los controles según la ISO 27001, se identificó que la Institución requiere de acciones inmediatas de mejora en los controles organizativos, de personas y físicos, mientras que existe una oportunidad de mejora en los controles tecnológicos, esto sugiere la necesidad de fortalecer las políticas internas, la formación del personal y la seguridad física, además de continuar mejorando las soluciones tecnológicas utilizadas.

En cuanto a los dominios de seguridad, la Institución tiene oportunidades de mejora en los dominios de identificar, proteger, detectar y recuperar, sin embargo, se requiere atención inmediata en el dominio de responder. Esto indica que, si bien existen áreas que pueden optimizarse en términos de identificación de riesgos, protección de activos, detección de incidentes y recuperación, la capacidad de respuesta inmediata a los incidentes es una prioridad.

Respecto a las capacidades operativas, se identificaron oportunidades de mejora en el aseguramiento de la seguridad de la información, la gestión de la identidad y del acceso, y la seguridad de los recursos humanos. Se requieren acciones inmediatas de mejora en la configuración segura, continuidad, gestión de amenazas y vulnerabilidades, gestión de eventos de seguridad de la información, gestión de activos, gobernanza, legal y cumplimiento, protección de la información y seguridad física.

En cuanto a los resultados de la evaluación de los controles según el Marco de Ciberseguridad NIST, se identifica que aunque hay áreas que están funcionando razonablemente bien, como la gestión de activos y la evaluación de riesgos, hay otras que necesitan mejoras significativas, especialmente la gobernanza y la estrategia de gestión de riesgos, asimismo la capacidad de recuperación para asegurar que la Institución pueda restaurar rápidamente sus operaciones normales después de un incidente de ciberseguridad, y la mitigación y la mejora continua.

Considerando los resultados obtenidos, esta Auditoría hace una observación especial, de la importancia de que la Institución asuma la Seguridad de la Información como un componente crítico para la integridad y resiliencia organizacional, si bien se han identificado y se están implementando acciones en el ámbito de la ciberseguridad, es esencial que la seguridad de la información reciba una atención especial.

La seguridad de la información no solo abarca la protección contra amenazas cibernéticas, sino también la salvaguardia de la confidencialidad, integridad y disponibilidad de los datos a través de controles físicos, administrativos y tecnológicos.

A pesar de los esfuerzos y mejoras en la ciberseguridad en la Institución, la seguridad de la información no ha recibido la misma atención y esto se refleja en las respuestas dadas por el equipo conformado para la atención de los instrumentos acá expuestos donde en reiteradas ocasiones hacen alusión a la ausencia del rol que asuma la dirección de esta materia. Esta disparidad puede dejar vulnerabilidades significativas en los procesos y sistemas de la Institución, exponiendo a la CCSS a riesgos innecesarios.

La Seguridad de la Información debe abordarse de manera integral, asegurando que todos los aspectos, desde la gestión de activos y la protección de datos hasta la formación del personal y la gestión de incidentes, estén cubiertos, de ahí la importancia que la Institución valore la asignación de ese rol de Oficial de Seguridad de la Información, que asegure una gestión adecuada y holística donde tenga la responsabilidad de desarrollar y ejecutar estrategias de Seguridad, coordinar la gestión de riesgos, supervisar el cumplimiento normativo, responder incidentes y especialmente promover la cultura de la Seguridad de la Información.

Lo anterior, asimismo fue externado por el equipo de trabajo conformado para la atención del requerimiento que originó este producto de Auditoría, donde en el oficio GG-DTIC-4270-2024 del 3 de julio de 2024, dirigido al Máster Robert Picado Mora, subgerente de la DTIC, el Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática indicó:

> *"Es importante señalar que, el equipo de trabajo externa la necesidad institucional de establecer una unidad que se encargue de gestionar la gobernanza y crear una cultura hacia la seguridad de la información y los datos institucionales. Con ello, nombrar lo que se conoce como el Oficial de la Seguridad de la Información (CISO), que tendrá la responsabilidad de dirigir al personal de la Institución en la identificación, desarrollo, implementación y mantenimiento de los procesos y actividades para reducir los riesgos de la información y los datos institucionales. Igualmente, de responder a los incidentes, establecer normas y controles apropiados, y dirigir en el establecimiento y aplicación de políticas y procedimientos para garantizar la seguridad y privacidad de los datos, entre otros.*
>
> *Adicionalmente, llama la atención del equipo de trabajo conformado para la atención de asuntos relacionados con la seguridad de los datos y la información, que la mayoría son profesionales en tecnologías de información y comunicaciones, limitándose la participación de la administración, lo que disminuye la observación de estos temas por parte de la misma y la creación de una cultura hacia estos temas tan importantes, como lo es, la seguridad de la información y los datos en los procesos y actividades institucionales, tema que van más allá, de lo que es la ciberseguridad".*

Sobre esta temática, la Auditoría Interna en diversos productos, ha evidenciado la necesidad de que la Seguridad de la Información sea asumido institucionalmente de forma integral, de tal forma que no sea un tema delegado a la Dirección de Tecnologías de Información y Comunicaciones, si no por el contrario, exista una participación de todas las gerencias de la Institución, como dueños de los procesos de negocio que se gestionan en la operativa, importantes volúmenes de información que deben ser protegidos y resguardados.

En esta línea, es importante mencionar que el 3 de noviembre de 2022, mediante oficio DFOE-CAP-3224 suscrito por la M. Sc. Jessica Víquez Alvarado, gerente de área de Fiscalización Operativa para el Desarrollo de Capacidades de la Contraloría General de la República, remitió a la Máster Marta Eugenia Esquivel Rodríguez, presidenta Ejecutiva de la CCSS, los resultados del nivel de aplicación de prácticas de Seguridad de la Información en las instituciones públicas, donde el ente Contralor identificó que la CCSS se encuentra en un **nivel básico** en esta materia, lo que refleja necesidad de implementar prácticas que fortalezca la gestión de la seguridad de la información.

Por todo lo anterior, es de importancia que se efectúen los esfuerzos necesarios, para llevar a cabo las acciones correspondientes para fortalecer las estrategias en torno a la Seguridad de la Información y la Ciberseguridad a nivel Institucional, considerando los riesgos inherentes en torno a esta materia que podría afectar la Institución.

Así las cosas, esta Auditoría previene y advierte de la situación indicada en el presente oficio, con el propósito de que sea visto en el Consejo Tecnológico Institucional, se tomen las acciones correspondientes, para minimizar o eliminar la materialización de riesgos asociados a la Seguridad de la Información y Ciberseguridad, por lo que se adjuntan los instrumentos: 1. Herramienta GSI ISO 27001 y 2. Checklist NIST, para el análisis correspondiente y la atención especialmente de aquellas respuestas donde la Institución obtiene una cumplimiento nulo o parcial en el caso de la ISO 27001 y una valoración de parcial y riesgo informado para las NIST.

Queda bajo exclusiva responsabilidad de esa Administración Activa, garantizar el monitoreo y mejoramiento continuo, de los mecanismos de control instaurados en torno a la situación y los riesgos advertidos; razón por la cual deben remitir a esta Auditoría en el término de **10 días hábiles** un plan de acción anexado al presente, con las acciones a ejecutar para la atención de los riesgos advertidos; cuyo plazo de atención de esta advertencia se consigna en **4 meses** a partir de la comunicación de este oficio.

Es necesario recordar la importancia de la confidencialidad, integridad e integralidad de la información que contiene este oficio y sus anexos, ya que el contenido de la documentación aportada tiene evidencia de las debilidades en materia de Seguridad de la Información y Ciberseguridad, que pueden ser utilizadas por ciberdelincuentes para efectuar un ataque a la institución.

Finalmente, se realiza un atento recordatorio sobre lo establecido en el artículo No. 17 de la Ley General de Control Interno No. 8292, en el cual se hace énfasis en la atención con prontitud de los hallazgos u observaciones de la Auditoría por parte de la administración activa.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.08.12 15:10:43 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

Anexos(3)

1. Herramienta GSI Consolidado Revisado AI
2. Checklist NIST CSF 1.1 Revisado AI
3. Plan de acción para atención del riesgo

C. Máster Vilma Campos Gómez, gerente a.i., Gerencia General -1100.
Doctor Alexander Sánchez Cabo, gerente a.i., Gerencia Médica-2901.
Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera -1103
Máster Gabriela Artavia Monge, 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.
Máster Jaime Barrantes Espinoza, gerente, Gerencia Pensiones-9108.
Ingeniera Susan Peraza Solano, directora, Dirección de Planificación Institucional-2902.
Auditoría-1111

Referencia: ID-121219