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

AD-AATIC-063-2022
1 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

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

Estimado señor:

ASUNTO: Oficio de Advertencia sobre gobierno y gestión de la ciberseguridad en la CCSS.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo del Área de Tecnologías de Información y Comunicaciones de esta Auditoria, para el período 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa el avance de la revisión efectuada sobre aspectos vinculados con gobernanza y gestión de la ciberseguridad Institucional. Lo anterior al amparo del marco regulatorio vigente aplicable, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa Administración.

Las tecnologías de información y comunicaciones han potenciado la mejora en el funcionamiento y prestación de servicios a la ciudadanía mediante aplicaciones y sistemas de información que han transformado procesos, tanto en salud, pensiones, como en la gestión administrativa y financiera en la institución. Adicionalmente, la presencia de servicios digitales en plataformas y las aplicaciones móviles han ido incrementando para satisfacer necesidades y requerimiento de los usuarios.

Lo anterior, hace necesario la evolución y reforzamiento de los esquemas de seguridad de la información tradicionales a un modelo de seguridad integral propiciado desde la Alta Direccion. En ese sentido, la Ciberseguridad busca la protección de los activos mediante el tratamiento de amenazas que ponen en riesgo los datos que son procesados, almacenados y utilizados por los sistemas informáticos y soluciones tecnológicas que son transportadas mediante redes de datos a lo largo y ancho del territorio.,

Desde hace varios años la ciberseguridad ha sido un desafío para las organizaciones, debido la existencia de múltiples amenazas y que cada día aparecen nuevas formas, siendo las más conocidas: Ransomware entendiendo este concepto como una especie de “secuestro de información” en el que un malware[1] encripta archivos y datos y pide un rescate para descifrarlos y desbloquearlos, el Phising, el cual es la suplantación de identidad a través de un correo electrónico en la que alguien se hace pasar por alguien más, usualmente entidades importantes como bancos, para robar información como contraseñas o datos.

En lo que respecta a ciberataques detectados a nivel mundial, Costa Rica se posicionó en el puesto No. 105 en el ranking de países atacados, lo anterior según los datos emitidos el 13 de junio del presente año por la empresa dedicada a la seguridad informática Kaspersky Lab, adicionalmente, se registró el aumentó de 2.000 a 4.500 embestidas diarias posterior al 18 de abril del 2022, cuando se dio a conocer la noticia del ataque a los sistemas del Ministerio de Hacienda.

[1] Se refiere a código malicioso, programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información. Es un acrónimo del inglés de malicious software.

De acuerdo con información de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), la CCSS detecta una cantidad importante de ataques cibernéticos, los cuales se detallan a continuación:

Tabla No. 1
Ciberataques a la Caja Costarricense de Seguro Social detectados por la DTIC

Periodo de tiempo	Cantidad de ataques
Anual	47 982 165
Mensual	3 998 513
Diario	133 283
Hora	5 553

Fuente-: Dirección de Tecnologías de Información y Comunicaciones, junio 2022.

En línea con lo anterior, es importante la diferencia entre seguridad de la información y la seguridad informática, siendo que, la Seguridad Informática consiste en una definición formal de las medidas que aplican la gestión de TIC para garantizar la seguridad de la información dentro del ámbito de las responsabilidades que le corresponden sobre la protección de la infraestructura computacional y los elementos relacionados. Mientras que la seguridad de la información hace referencia al conjunto de medidas preventivas y reactivas para resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

En virtud de lo anterior, las organizaciones y en particular la CCSS debe protegerse de esos ataques y evitar que se generen eventos como los que se han presentado recientemente.

ANTECEDENTES

Licitación Abreviada No.2016LA-000003-1150 dio inicio al proyecto denominado *"Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS".*

La DTIC, mediante la Licitación Abreviada No.2016LA-000003-1150 dio inicio al proyecto denominado: *"Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS de servicios profesionales para el diseño de un Modelo Meta de Gobernanza de TIC y de Gobierno de Seguridad de la Información para la CCSS de servicios profesionales para el diseño de un Modelo Meta de Gobernanza de TIC y de Gobierno de Seguridad de la Información para la CCSS"*.

Análisis integral de brechas con respecto al proceso Gestionar los servicios de Seguridad

Durante el desarrollo de la Fase No.4 del proyecto de marras, se entregó el documento E4 denominado: *"Análisis integral de brechas"*, especificando a través de la tabla 36. *"Identificación y análisis de brechas con respecto al proceso Gestionar los servicios de seguridad"* el nivel de capacidad actual de la CCSS respecto al proceso DSS05 *"Gestionar los servicios de seguridad"* y el nivel de capacidad en ese momento de cero (Proceso incompleto).[2]

Adicionalmente, en el documento supra se determinaron diez hallazgos, los cuales se transcriben a continuación:

> "… *No existen mecanismos automatizados que apoyen en la detección y eliminación de software no licenciado instalado en los equipos de la red institucional, que comprometa la seguridad, integridad y disponibilidad de las soluciones tecnológicas.*

- *No existen mecanismos automáticos de control que garanticen que la información crítica disponible en medios finales como computadoras portátiles y terminales de trabajo, sea únicamente transferible a dispositivos de extracción confiables y autorizados.*

[2] Según COBIT existen 5 niveles para medir la capacidad: falta

- *Al no existir una clasificación clara de la información a nivel institucional, no se existe implementado un esquema de manejo y almacenamiento de la información diferenciado por el nivel de criticidad de los datos.*
- *No existen lineamientos apoyados en soluciones ni mecanismos automáticos implementados que garanticen la disponibilidad de la información almacenada en las terminales de trabajo como respuesta ante fallos en los equipos de usuario.*
- *No existen un procedimiento formal establecido que garantice que los privilegios, accesos y roles asignados a los usuarios de las soluciones y servicios TIC, corresponden al nivel de responsabilidad o rol institucional que desempeña en el puesto.*
- *No existen roles y responsabilidades dentro de la organización que garanticen la gestión adecuada de los derechos de acceso de los usuarios sobre las soluciones de negocio que se apoyan en componentes tecnológicos.*
- *No existen procedimientos formales implementados que garanticen el control de acceso físico autorización y supervisado a sitios donde se almacena y procesa información relevante para la prestación de servicios institucional.*
- *No existen procedimientos formales que apoyen en la gestión de incidentes relacionados a la seguridad de la información, que aborden los mecanismos y procedimientos para el reporte del problema, los procedimientos de atención, resolución, y recopilación de evidencias, y los mecanismos formales para comunicar sobre el incidente y las medidas tomadas para su resolución o mitigación.*
- *No existen mecanismos automáticos que apoyen en la detección de incidentes de seguridad, cuando los mismos suceden a través de canales, medios y procedimientos lícitos habilitados como soporte a un servicio institucional de negocio. (uso ventajoso no autorizado o mediante procedimientos no lícitos de los servicios y soluciones institucionales y tecnológicas).*
- *No existen mecanismos de seguridad informática formales estándar, que garanticen el aseguramiento de la operatividad de los equipos y dispositivos de tecnología médica y operativa."*

Plan de acción consolidado para el cierre de brechas

En lo concerniente a los entregables de la fase No. 5, mediante el documento E5 llamado *"Plan de Acción consolidado para el cierre de brechas"* de diciembre 2017, se establecieron las iniciativas de mejora inmediata, a corto, mediano y largo plazo, determinando en el apartado 5.1.3 *"Iniciativas a mediano plazo"*, cuya proyección de ejecución se indicó a 12 meses posterior a la finalización del Proyecto de Gobernanza, Gestión y Seguridad de la CCSS, específicamente en el eje de acción Seguridad de la Información la iniciativa denominada *"IMP15-Establecer el Plan Táctico de Ciberseguridad"*.

Licitación Abreviada N° 2019LA-000001-1150 "Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS"

En el 2019, la DTIC gestionó la Licitación Abreviada No. 2019LA-000001-1150 cuyo objeto contractual corresponde a *"Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS"* y constaba de la ejecución de cinco fases, las cuales se mencionan en la siguiente tabla:

Tabla N°2
Fases del Plan de Ciberseguridad para la CCSS

Fase	Objetivo
1. Planificación	Desarrollar el Plan del Proyecto y el mapa de ruta a seguir, mecanismos de control, riesgos y acciones para mitigar situaciones inesperadas.
2. Análisis Actual	Conocer la realidad actual de la Caja Costarricense de Seguro Social en torno a la ciberseguridad
3. Diseño de estado deseado	Definir el estado deseado de ciberseguridad de la Caja Costarricense de Seguro Social y como debería funcionar el Plan de Ciberseguridad con sus componentes clave para lograr el estado objetivo.

4. Brechas, riesgos y benchmarking	Identificar y documentar las brechas de ciberseguridad que existen para alcanzar el estado objetivo.
5. Hoja de ruta	Documentar la hoja de ruta que detalla los proyectos o iniciativas para alcanzar el servicio de ciberseguridad deseado.
6. Diseño de mejoras prioritarias	Diseñar y documentar las 10 iniciativas identificadas en la hoja de ruta diseñada en la fase anterior, elegidas por las Caja Costarricense de Seguro Social

Fuente: Elaboración propia basada en el documento PCS-ENT-001 "Plan Proyecto", junio 2022.

OBSERVACIONES

En ese sentido, como resultado del análisis efectuado respecto a la información suministrada por la Administración Activa, nos permitimos realizar las siguientes observaciones en torno a aspectos relacionados con el gobierno, gestión y operación de la ciberseguridad en la Institución:

1. Gobierno de TIC y de seguridad informática y de la información

La Institución no dispone de un modelo de gobierno de la seguridad informática a nivel institución, que direccione los objetivos estratégicos y la generación de valor en torno a este tema, contribuya a la mitigación de riesgos asociados y a que se disponga de capacidades de seguridad requeridas acorde con la dirección establecida, los servicios prestados y el ordenamiento jurídico.

Adicionalmente, es necesario el establecimiento de métricas que oriente la toma de decisiones y las inversiones en esta materia.

Al respecto, la firma contratada Price Water House Coopers (PwC), 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"*, identificó los siguientes hallazgos claves sobre la visión estratégica:

- 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.

Además, mediante el entregable denominado *"Informe de situación actual de la seguridad de las TIC"* del 25 de mayo del 2020, correspondiente a la Licitación Abreviada 2019LA-000001-1150 *"Servicios Profesionales para desarrollar un Plan de Ciberseguridad para la CCSS"*, se indicó las siguientes áreas de mejora relacionadas con el gobierno de ciberseguridad:

- Las iniciativas de gobernanza que alinean TIC y negocio en términos de inversiones y toma de decisiones se encuentran aún en fase de implementación por parte la Alta Administración.

- No existe ni se evalúa o monitorea el marco de gobierno de ciberseguridad.

En ese sentido, el 9 de junio de 2022, mediante oficio GG-DTIC-2892-2022, la Ing. Mayra Ulate Rodríguez, jefe del Área de Seguridad y Calidad de la Información (ASCI) de la DTIC, indicó a esta Auditoría la información asociada al nivel de avance de las iniciativas de ciberseguridad planteadas en la Contratación 2019LA-000001-1150.

Al respecto, se Indicó que los siguientes entregables correspondientes a las Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS (PCS-GI-01), se encontraba en fase de desarrollo.

- Roles y responsabilidades de ciberseguridad definidos formalmente.
- Recursos de ciberseguridad asignados de acuerdo con un enfoque en riesgos.

2. Sobre operación y gestión de la seguridad informática

Resulta necesario la definición de roles y responsabilidades para la operación y gestión de la ciberseguridad, procurando una separación de funciones que garantice no solo la posibilidad de efectuar análisis de las alertas, incidentes y vulnerabilidades identificadas, sino también acciones para gestionarlas, y no distraer los recursos que se encuentran a cargo del funcionamiento operativo.

Lo anterior, potencia la capacidad de planeación y ejecución de acciones tendientes a mitigar riesgos y a prevenir posibles ataques, pues hay mayor capacidad de prevención. Adicionalmente, permite disponer de indicadores que pueden ser evaluados y gestionados en concordancia con la estrategia global de ciberseguridad, promoviendo el principio de rendición de cuentas y transparencia a través de métricas disponibles en torno a la seguridad

3. Sobre la estrategia integral de ciberseguridad

La Institución no dispone de una estrategia integral de ciberseguridad, que permita el aprovechamiento de los recursos disponibles y la orientación de esfuerzos en torno al logro de los objetivos estratégicos definidos en esta materia, así como la promoción de una cultura enfocada en la confiabilidad integridad, privacidad y seguridad de activos tecnológicos y de los datos.

Lo anterior, con el fin de posicionar la gestión de seguridad, tanto a nivel central como en el ámbito local y los centros de datos que no se encuentran ubicados en el Parque Tecnológico CODISA[3].

Al respecto, resulta importante señalar lo identificado en el entregable PCS-ENT-002 *"Informe de situación actual de la seguridad de las TIC"* de la Licitación Abreviada 2019LA-000001-1150 *"Servicios profesionales para desarrollar un Plan de Ciberseguridad de la CCSS"*, específicamente en aparato dedicado a las áreas de mejora detectadas del Dominio *"Estrategia, gobernanza y gestión"*, que señalan:

"

(…) No existe una estrategia de ciberseguridad ni hoja de ruta."

En ese sentido, la Ing. Mayra Ulate Rodríguez, Jefe del ASCI de la DTIC, remitió oficio GG-DTIC-2892-2022 del 9 de junio del 2022, a esta Auditoría indicando el nivel de avance de las iniciativas de ciberseguridad planteadas en la Fase No. 6 de la licitación de marras.

Al respecto, indicó que, los entregables correspondientes a las Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS (PCS-GI-01), se encontraban en fase de desarrollo, destacando el siguiente:

- Estrategia de ciberseguridad formalizada con una revisión cada 5 años y la hoja de ruta revisada anualmente

[3] Empresa costarricense que ofrece productos y servicios de tecnologías de información para los sectores: financiero, gobierno y privado. Ofrece soluciones de Centro de Datos, Almacenamiento en la Nube, Software, entre otros.

4. Sobre el Monitoreo de Seguridad de la Institución 24/ 7 y Centro de Operaciones de Seguridad (SOC)

La CCSS no cuenta con un Centro de Operaciones de Seguridad (SOC), que se encargue de las operaciones de seguridad de tecnologías de información y comunicación de forma centralizada, permitiendo el monitorear y supervisión en tiempo real todos los elementos y datos, los cuales podrían afectar la seguridad de la infraestructura e información, así como visualizar integralmente amenazas, incidentes y vulnerabilidades.

En ese orden de ideas, no se dispone de recurso asignado por parte de la Subárea de Seguridad de TI, exclusivo para monitorear eventos de seguridad, así como tampoco se han definido equipos de trabajo dedicados a realizar análisis de vulnerabilidades, pruebas de penetración y evaluaciones de seguridad web.

Sobre este particular, esta Auditoría tuvo conocimiento sobre la ejecución de evaluaciones relacionadas con algunos de los temas mencionados previamente, lo anterior con apoyo de procesos de contratación de servicios tercerizados como por ejemplo la empresa Deloitte & Touché.

En ese sentido, el 9 de junio del 2022, mediante oficio GG-DTIC-2892-2022, la Ing. Mayra Ulate, jefe del ASCI de la DTIC, indicó a esta Auditoría el nivel de avance de las iniciativas de ciberseguridad planteadas en la Contratación 2019LA-000001-1150 *"Servicios profesionales para desarrollar un Plan de Ciberseguridad de la CCSS"*.

Al respecto, la Ing. Ulate Rodríguez, indicó que las iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS (PCS-GI-15), se encontraba en fase de desarrollo, destacando el comienzo de la iniciativa denominada *"Diseño e implementación de un SOC para la CCSS."* en el segundo semestre del 2022 con una duración de 38 meses.

5. Control de activos TIC

Es importante que la institución registre todos los activos de tecnologías de información y comunicaciones y además se clasifiquen según criticidad considerando el impacto en los servicios que presta y el rol de cada uno de ellos, así como la integración entre los diferentes elementos de hardware y software.

En ese sentido, el Informe de situación actual de la seguridad de las TIC, de la contratación Servicios Profesionales para desarrollar un Plan de Ciberseguridad para la CCSS, Licitación Abreviada 2019LA-000001-1150, indicó en torno a áreas de mejora relacionadas con este aspecto, lo siguiente:

- Las herramientas y controles tecnológicos desplegados para la protección de los activos de información se integran de forma limitada y no proporcionan una visión integral de la Institución, en parte porque estas herramientas y tecnologías automatizadas no se aprovechan al máximo.

- No existen procesos formales documentados que se comuniquen en toda la Institución para definir y clasificar los recursos de red o de sistemas, asignar niveles de importancia a los recursos e identificar posibles amenazas para cada uno.

6. Sobre los protocolos utilizados

Esta Auditoría efectuó la consulta sobre los protocolos y procedimientos de seguridad aprobados para el manejo de incidentes como el de tráfico anómalo.

Al respecto, la Administración, mediante oficio GG-DTIC-1725-2022 del 28 de marzo de 2022, señaló lo siguiente:

"*Protocolo uno utilizado:*

• Protocolo "DSS02-PT-003 Protocolo de incidencia Lentitud General en Servicios v1.2.pdf" adjunto, ya que se atiende este tipo de casos en la Mesa de Servicios TIC, que es la cara principal de la gestión de servicios TIC. Este protocolo se encuentra en este momento en proceso de aprobación y divulgación de acuerdo con los lineamientos establecidos por la DTIC, para este tipo de documentos.

Protocolo dos utilizado:

• Protocolo de Servicios tercerizados: donde tenemos acceso al protocolo Deloitte para Gestión de Eventos de Seguridad TI. Este protocolo es solicitado dentro del proceso de contratación a la empresa adjudicada, el mismo no se brinda por ser un documento confidencial…"

De lo anterior, se concluye que el protocolo utilizado DSS02-PT-003 *"Protocolo de incidencia Lentitud General en Servicios v1.2"*, no se encuentra aprobado, ni divulgado a los actores correspondientes, lo cual a criterio de esta Auditoría representa riesgos asociados con ambiente de control, suficiencia del contenido del protocolo, así como la aplicación y comprensión de estos.

Por lo tanto, es fundamental que la Institución disponga de protocolos aprobados y divulgados a los actores requeridos para su ejecución, conforme los niveles de seguridad correspondientes, los cuales deben desarrollarse para los posibles eventos, amenazas o ataques que se presenten.

7. Sobre el proyecto de seguridad perimetral

El 30 de julio del 2020, mediante oficio GG-DTIC-4439-2020, la DTIC efectuó solicitud de información relacionada con el inicio del proceso de contratación para la adquisición de *"Solución Institucional de Seguridad Perimetral"* bajo la figura de seguridades calificadas, lo anterior según lo dispuesto en el artículo 139 inciso h del Reglamento a la Ley de Contratación Administrativa.

En ese sentido, de acuerdo con esa Direccion, la compra de marras forma parte de la atención de brechas identificadas en seguridad TI durante el desarrollo del Proyecto de Ciberseguridad a través del diagnóstico, análisis de vulnerabilidades y riesgos, basados en mejores prácticas y estudio de tendencias.

Al respecto, la DTIC tramitó la contratación directa No. 2021CD-000007-0001101150, cuyo objeto es *"Solución Tecnológica para Seguridad Perimetral"*, la cual fue aprobada por la Junta Directiva el 13 de enero 2022 a la empresa Soluciones Seguras SSCR Sociedad Anónima. Lo anterior dio origen al contrato No. 0432022115000009-00, refrendado por la Dirección Jurídica el 7 de marzo de 2022.

En la siguiente tabla se detallan los ítems adjudicados con su respectivo monto:

Tabla No. 3
Ítems de la Contratación Directa No. 2021CD-000007-0001101150
"Solución Tecnológica para Seguridad Perimetral"

No. Ítem	Descripción	Cantidad	Monto
1	Equipo Firewall de próxima generación NGFW (Gateway), con funciones de seguridad perimetral, memoria RAM de 32 GB, mínimo de puertos: 10 slot de 1 GB, 4 de 10 GB de fibra (fase 1 - CODISA).	4 uds	$ 240.896
2	Equipo maestro para administración de Firewall, de próxima generación, con mínimo 8 puertos de 100 GB de fibra y 48 de 10 GB, cables: 10 GBE (DAC) de 3m. (Fase 1 - CODISA).	2 uds	$ 76.354
3	Licencias de software para muro de fuegos de nueva generación. (Fase 1 - CODISA).	4 uds	$ 135.596

4	Equipo de gestión para Firewall de próxima generación con capacidad de administración para 75 equipos, memoria RAM de 96gb, 24 TB HDD, 2x fuentes de poder ac (Fase 1 - CODISA).	2 uds	$ 72.560
5	Sistema de reportería para Firewall de próxima generación. última versión. vigencia por un año. capacidad de administración para 75 equipos, memoria RAM de 96GB, Disco Duro: 24 TB HDD / Servidor (Fase 1 - CODISA).	1 u	$ 31.280
6	Software herramienta de diagrama lógico de equipos de seguridad, con capacidad de análisis de tráfico. (Fase 1 - CODISA).	1 u	$ 18.418
7	Servicio de ingeniería para el análisis, rendimiento y solución de problemas para equipo de tecnología de la información y comunicación (TIC). (Fase 1 - CODISA).	48 meses	$ 206.500
8	Servicio de ingeniería para el análisis, rendimiento y solución de problemas para equipo de tecnología de la información y comunicación (TIC). (Fase 1 - CODISA).	8 semestres	$ 48.000
9	Equipo Firewall de próxima generación NGFW (Gateway), con funciones de seguridad perimetral, memoria RAM de 32 GB, mínimo de puertos: 10 SLOT DE 1 GB, 4 DE 10 GB DE FIBRA (Fase 2 – Sitio Alterno).	4 uds	$ 240.896
10	Equipo maestro para administración de Firewall, de próxima generación, con mínimo 8 puertos de 100 GB DE FIBRA Y 48 de 10 GB, cables: 10 GBE (DAC) de 3M (Fase 2 – Sitio Alterno).	2 uds	$ 76.354
11	Licencias de software para muro de fuegos de nueva generación (Fase 2 – Sitio Alterno).	4 uds	$ 135.596
12	Servicio de ingeniería para el análisis, rendimiento y solución de problemas para equipo de tecnología de la información y comunicación (TIC).	48 meses	$ 159.550
13	Servicio de mantenimiento preventivo y correctivo del equipo de cómputo: Se refiere a las clasificaciones de servicios mantenimientos preventivos de hardware y software de equipos de seguridad informática (Fase 2 – Sitio Alterno).	8 semestres	$ 48.000
		Total	$ 1.490.000

Fuente: Elaboración propia basada en el Contrato No. No. 0432022115000009-00 de la Contratación Directa No. 2021CD-000007-0001101150.

Al respecto, es fundamental disponer de un plan de trabajo con responsabilidades, plazos y fechas, de forma tal que se disponga de la solución perimetral instalada a la brevedad y con ello minimizar riesgos en torno a la capacidad institucional actual.

8. Sobre las iniciativas del Plan de ciberseguridad

Mediante la revisión efectuada del respaldo documental asociada a los entregables de la contratación 2019LA-000001-1150 *"Servicios profesionales para desarrollar un Plan de Ciberseguridad para la CCSS"*, se identificaron los siguientes aspectos:

8.1. Sobre la fecha de inicio y avance de las iniciativas a desarrollar para subsanar brechas de Ciberseguridad

El documento PCS-ENT-029 *"Plan de Ciberseguridad"* elaborado el 14 de diciembre 2020, especifica en el apartado 7.6.3 *"Priorización de los grupos de iniciativas y documentación de la hoja de ruta"*, el establecimiento de 23 iniciativas priorizadas para subsanar brechas de ciberseguridad detectadas a nivel Institucional, lo anterior de conformidad con la aplicación de un esquema de puntuaje, así como el análisis y estado actual de la CCSS realizado en las fases No. 2 y No. 4 de la contratación de marras.

En virtud de lo anterior, esta Auditoría solicitó información sobre la fecha de inicio y estado de implementación de dichas iniciativas, obteniendo como respuesta el oficio GG-DTIC-2892-2022 del 9 de junio del presente año, en el cual se identificó que solamente un proyecto registra un avance de 100%, uno presenta un 85%, ocho se encuentran con un porcentaje de ejecución entre el 10% y 30%, y finalmente, trece tienen consignado un 0% de avance.

En la siguiente tabla se detallan los aspectos relacionados con las fechas de inicio propuestas y actuales, así como el porcentaje de avance y estado de cada iniciativa:

Tabla No. 4
Iniciativas priorizadas para subsanar las brechas de ciberseguridad en la CCSS

Código y nombre de la iniciativa	Fecha de inicio propuesta	Fecha de Inicio (DTIC)	Estado de iniciativa	Porcentaje de avance actual
PCS-GI-01 Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Primer semestre 2021	Segundo semestre 2022	En desarrollo	85%
PCS-GI-02 Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Primer semestre 2021	Segundo semestre 2021	En desarrollo	10%
PCS-GI-03 Iniciativas para la retroalimentación de las vulnerabilidades identificadas para el mejoramiento de la seguridad física y ambiental de los sitios que se analizaron en la fase 2 de situación actual.	Primer semestre 2021	Primer semestre 2022	En desarrollo	28%
PCS-GI-04 Iniciativas para la definición de los servicios de ciberseguridad que serán ofrecidos a través de la mesa de servicio de la CCSS.	Primer semestre 2021	Primer semestre 2021	En desarrollo	100%
PCS-GI-05 Iniciativas para la creación de un modelo de capacitación y especialización continua en Ciberseguridad y su integración con el Plan de Capacitación existente en la DTIC.	Primer semestre 2021	Segundo semestre 2022	No iniciado	0%
PCS-GI-07 Iniciativas para la implementación de la gestión del riesgo cibernético.	Primer semestre 2021	Segundo semestre 2022	En desarrollo	18%
PCS-GI-10 Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Primer semestre 2021	Segundo semestre 2021	En desarrollo	20%
PCS-GI-15 Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Primer semestre 2021	Segundo semestre 2022	En desarrollo	15%
PCS-GI-23 Iniciativas para el fortalecimiento de la seguridad perimetral	Primer semestre 2021	Primer semestre 2022	No iniciado	0%
PCS-GI-19 Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.	Segundo semestre 2021	Primer semestre 2023	No iniciado	0%
PCS-GI-20 Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.	Segundo semestre 2021	Segundo semestre 2023	No iniciado	0%
PCS-GI-12 Iniciativas para el fortalecimiento de la identidad y gestión de acceso.	Primer semestre 2022	Primer semestre 2023	No iniciado	0%
PCS-GI-16 Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software.	Primer semestre 2022	Primer semestre 2023	No iniciado	0%
PCS-GI-09	Segundo semestre 2022	Segundo semestre 2022	No iniciado	0%

Iniciativas para la implementación de la gestión de vulnerabilidades y parches.				
PCS-GI-13 Iniciativas para la gestión del acceso privilegiado en los sistemas de la CCSS.	Primer semestre 2023	Primer semestre 2024	En desarrollo	15%
PCS-GI-17 Iniciativas para la simulación de ataques y pruebas de seguridad	Segundo semestre 2023	Segundo semestre 2023	En desarrollo	0%
PCS-GI-11 Iniciativas para la implementación de la gestión de la seguridad de los endpoint.	Primer semestre 2024	Primer semestre 2022	En desarrollo	20%
PCS-GI-18 Iniciativas para la implementación de la gestión de la seguridad en la nube.	Primer semestre 2024	Segundo semestre 2024	No iniciado	0%
PCS-GI-22 Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC	Primer semestre 2024	Segundo semestre 2024	No iniciado	0%
PCS-GI-14 Iniciativas para el establecimiento e implementación de las líneas base de seguridad.	Segundo semestre 2024	Segundo semestre 2024	No iniciado	0%
PCS-GI-21 Iniciativas para el aprovechamiento de los acuerdos nacionales e internacionales para potenciar el conocimiento y desarrollo de la ciberseguridad en la CCSS.	Segundo semestre 2024	Segundo semestre 2024	En desarrollo	25%
PCS-GI-06 Iniciativas para el desarrollo de una estrategia de respaldos institucional.	Primer semestre 2025	Primer semestre 2025	No iniciado	0%
PCS-GI-08 Iniciativas para la definición de una arquitectura de ciberseguridad que se alinee con los objetivos de la DTIC.	Primer semestre 2025	Primer semestre 2025	No iniciado	0%

Fuente: Elaboración propia basada en los documentos PCS-ENT-029 "Plan de Ciberseguridad" y GG-DTIC-2892-2022, junio 2022.

8.2. Sobre la modificación de las fechas de inicio propuestas en la hoja de ruta

Se identificó la modificación de las fechas de inicio propuestas de 15 de las 23 iniciativas prioritarias para disminuir las brechas de ciberseguridad, lo anterior según lo señalado en el documento PCS-ENT-029 "Plan de Ciberseguridad" y el oficio GG-DTIC-2892-2022 del 9 de junio del presente año.

En la siguiente tabla se puede observar el detalle:

Tabla No. 5
Iniciativas que presentan diferencias en la fecha de inicio respecto a lo establecido en documento DCS-ENT-029 "Plan de Ciberseguridad"

Código y nombre de la iniciativa	Fecha de inicio propuesta	Fecha de Inicio según DTIC
PCS-GI-01 Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Primer semestre 2021	Segundo semestre 2022
PCS-GI-02 Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Primer semestre 2021	Segundo semestre 2021
PCS-GI-03 Iniciativas para la retroalimentación de las vulnerabilidades identificadas para el mejoramiento de la seguridad física y ambiental de los sitios que se analizaron en la fase 2 de situación actual.	Primer semestre 2021	Primer semestre 2022
PCS-GI-05 Iniciativas para la creación de un modelo de capacitación y especialización continua en	Primer semestre 2021	Segundo semestre 2022

Ciberseguridad y su integración con el Plan de Capacitación existente en la DTIC.		
PCS-GI-07 Iniciativas para la implementación de la gestión del riesgo cibernético.	Primer semestre 2021	Segundo semestre 2022
PCS-GI-10 Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Primer semestre 2021	Segundo semestre 2021
PCS-GI-15 Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Primer semestre 2021	Segundo semestre 2022
PCS-GI-23 Iniciativas para el fortalecimiento de la seguridad perimetral	Primer semestre 2021	Primer semestre 2022
PCS-GI-19 Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.	Segundo semestre 2021	Primer semestre 2023
PCS-GI-20 Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.	Segundo semestre 2021	Segundo semestre 2023
PCS-GI-12 Iniciativas para el fortalecimiento de la identidad y gestión de acceso.	Primer semestre 2022	Primer semestre 2023
PCS-GI-16 Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software.	Primer semestre 2022	Primer semestre 2023
PCS-GI-13 Iniciativas para la gestión del acceso privilegiado en los sistemas de la CCSS.	Primer semestre 2023	Primer semestre 2024
PCS-GI-18 Iniciativas para la implementación de la gestión de la seguridad en la nube.	Primer semestre 2024	Segundo semestre 2024
PCS-GI-22 Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC	Primer semestre 2024	Segundo semestre 2024

Fuente: Elaboración propia basada en los documentos PCS-ENT-029 “Plan de Ciberseguridad” y GG-DTIC-2892-2022, junio 2022.

Adicionalmente, llama la atención de esta Auditoría el establecimiento de las fechas de inicio de las 23 iniciativas definidos “por semestre”, aspecto que ocasiona limitaciones sobre la determinación exacta del atraso presentado en la ejecución de cada proyecto.

8.3. Sobre la revisión, análisis y priorización de las iniciativas

Teniendo en consideración la situación actual de la Institución respecto al ataque cibernético sufrido el pasado 31 de mayo de 2022, así como el establecimiento de la hoja de ruta que permitan el cierre de brechas a nivel de ciberseguridad, es necesario que la Administración valore nuevamente la priorización efectuada de las 23 iniciativas definidas en el entregable PCS-ENT-029 de la Licitación 2019LA-000001-1150, lo anterior considerando aspectos vinculados con los recursos financieros y humanos requeridos, así como el impacto y los riesgos asociados.

Además, resulta importante tener en cuenta, dentro de dicha valoración, aspectos como los prerrequisitos y/o dependencia entre las iniciativas establecidas en la hoja de ruta entregada por la empresa consultora, el lapso que conlleva la ejecución de etapas vinculadas con procesos contractuales y los respectivos atrasos en el caso de los proyectos que así lo requieran previo a su implementación.

A continuación, se detallan las iniciativas cuyo inicio se proyectó a partir del segundo semestre del 2023:

Tabla No. 6
Iniciativas con proyección de inicio posterior al segundo semestre 2023

Iniciativas	Fecha proyectada de inicio (DTIC)	Tiempo de desarrollo
PCS-GI-06 Iniciativas para Desarrollo de una estrategia de respaldo institucional	Primer semestre 2025	No disponible
PCS-GI-18 Iniciativas para la implementación de la gestión de la seguridad en la nube.	Segundo semestre 2024	6 meses
PCS-GI-17 Iniciativas para la simulación de ataques y pruebas de seguridad	Segundo semestre 2023	16 meses
PCS-GI-08 Iniciativas para la definición de una arquitectura de ciberseguridad que se alinee con los objetivos de la DTIC	Primer semestre 2025	No disponible
PCS-GI-20 Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas	Segundo semestre 2023	12 meses

Fuente: Elaboración propia basada en los documentos PCS-ENT-029 "Plan de Ciberseguridad" y GG-DTIC-2892-2022, junio 2022.

9. Sobre evaluaciones efectuadas en ciberseguridad y seguridad de la información

Uno de los entregables de la contratación N° 2019LA-000001-1150 *"Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS"* fue el documento PCS-ENTR-002 *denominado "Informe de situación actual de la seguridad de las TIC"* de mayo 2020, en el cual se señaló entre otras cosas, las áreas de mejora detectadas en la CCSS de acuerdo con los ocho dominios de ciberseguridad.

A continuación, se menciona la cantidad de aspectos de mejora detectados por dominio:

Tabla No. 7
Cantidad de áreas de mejora detectadas por dominio de ciberseguridad

Dominio	Cantidad de áreas de mejora
Estrategia, gobernanza y gestión	17
Arquitectura y servicios de seguridad	14
Inteligencia de amenazas y gestión de vulnerabilidades	17
Gestión de identidad y acceso	17
Privacidad y protección de la información	16
Gestión de incidentes y crisis	14
Gestión de riesgo y cumplimiento	15
Tendencias emergentes e innovación	7
Análisis de elementos adicionales	88
Total	205

Fuente: Elaboración propia basada en el documento PCS-ENTR- 002 "Informe de situación actúa de la seguridad de las TIC", junio 2022.

En virtud de lo anterior, la administración debe poner énfasis a las diferentes oportunidades de mejora detectadas por la firma consultora PwC durante la ejecución de la Licitación Abreviada 2019LA-000001-1150, considerando aspectos vinculados con la valoración y el análisis y priorización en la atención, así como el establecimiento de estrategias para para cerrar las brechas detectadas, logrando la minimización de riesgos en torno a cada una de los dominios correspondientes, vulnerabilidades y ataques futuros.

Consideraciones normativas

La Ley General de Control Interno, en artículo No. 8 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 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."*

Ese cuerpo normativo también señala en el apartado XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, lo siguiente:

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

La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.

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

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

"establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.".

"evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.".

"probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.".

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".

Por su parte, las Normas de Control Interno para el Sector Público señalan en el inciso 5.7.4 Seguridad que:

"Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."

Consideraciones finales

Tal y como ha venido señalando este Órgano de Fiscalización y Control, la CCSS, depende de la información, sistemas y soluciones tecnológicas que soportan su gestión y permiten la prestación de los servicios a la ciudadanía, de ahí la necesidad de disponer, entre otros aspectos, de un marco de seguridad informática y de seguridad de la información que incluya normativa, políticas, procesos, herramientas y equipos, para prevenir y asegurar la disponibilidad y capacidad de la plataforma tecnológica, minimizando la materialización de riesgos asociados a amenazas, incidentes de seguridad y ciberseguridad, así como ataques de los cuales ha sido víctima recientemente con un impacto tanto en la atención de los usuarios a nivel nacional como en el desempeño y ejecución de los procesos internos.

En virtud de lo anterior, la Institución debe planificar la gestión de continuidad del negocio en cada uno de los procesos de salud, pensiones y recaudación patronal que tiene a cargo para evitar que las actividades sustantivas sean interrumpidas.

En virtud de lo expuesto, se previene y advierte a la Administración sobre los aspectos mencionados en el presente oficio, con el propósito de evitar la materialización de riesgos asociados al gobierno, gestión y operación de la seguridad de la información e informática a fin de prevenir y mitigar el impacto asociado a ataques de ciberseguridad y en la continuidad de los servicios, así como coadyuvar al cumplimiento de los objetivos institucionales y paralelamente innovar en la mejora continua de los procesos de trabajo.

Por lo tanto, esta Auditoría Interna en el ejercicio de las competencias de control y fiscalización, establecidas en el ordenamiento jurídico aplicable, procede a emitir el presente oficio, con el objetivo de proporcionar un avance sobre aspectos vinculados con gobernanza y gestión de ciberseguridad a nivel institucional.

En virtud de lo expuesto anteriormente, los aspectos detectados podrían generar la eventual apertura de procedimientos administrativos según corresponda, por lo que, en aras de la seguridad jurídica de las evaluaciones subsecuentes, **se solicita mantener la debida confidencialidad sobre las observaciones esbozados en el presente oficio,** según lo establecido en el Artículo 6º de la Ley General de Control Interno No.8292

Finalmente, se realiza un 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 de la Auditoría por parte de la administración activa.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada, en el **plazo de un mes** a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.04 12:18:00 -06'00'

Lic. Olger Sánchez Carrillo.
Auditor

OSC/RJS/RAHM/IMS/GMP/lbc

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