ATIC-0095-2023
4 de diciembre de 2023

RESUMEN EJECUTIVO

El presente estudio se realizó de conformidad con el Plan Anual Operativo 2023 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión y el control que realiza la administración activa en torno al avance en la implementación de las iniciativas derivadas del Plan de Ciberseguridad.

Los resultados del estudio permitieron identificar que la ejecución de la hoja de ruta del Plan de Ciberseguridad no es gestionada como un proyecto o programa de proyectos, donde se definan actividades que valoren aspectos de alcance, tiempo, presupuesto y uso óptimo de los recursos, asimismo, se realice la medición del desempeño, e identificación de mejora, lo anterior mediante el uso de indicadores que permitan controlar el nivel del logro de las metas planteadas.

Se identificó que el Plan de Ciberseguridad vigente se encuentra integrado al AGEDI como mecanismo de control y seguimiento del proyecto, no obstante, este se incluyó en la Agenda con el alcance orientado a la definición de dicho plan, por lo que al estar formalizado el entregable, dicho proyecto aparece actualmente con un nivel de cumplimiento del 100%, quedando pendiente la inclusión de la hoja de ruta.

Respecto al avance de las 23 iniciativas de la hoja de ruta del Plan de Ciberseguridad, se identificó el incumplimiento en la implementación de estas cuyo plazo estimado de ejecución estaban definidos para el 2021, 2022 y 2023, asimismo se observó la atención de otra iniciativa que por el contrario estaba contemplada para el I Semestre del 2025.

Se identificaron oportunidades de mejora en los controles implementados por parte de la Administración Activa, en torno a la gestión de la ejecución del Plan de Ciberseguridad y su hoja de ruta respecto los informes periódicos sobre el avance en la implementación, definición de roles y responsabilidades.

En cuanto al Plan Reforzado de Ciberseguridad, se evidenció que no se ha aprobado formalmente por parte del Consejo Tecnológico, aunado a que no se identificó el cumplimiento de las etapas definidas en la normativa institucional para el aval por parte de ese Órgano Colegiado, de tal forma que se garantice que la Institución dispone de los recursos para llevar a cabo la materialización del Plan reforzado y las iniciativas establecidas.

Aunado a lo anterior, se determinó que la DTIC ha identificado como limitante para el cumplimiento efectivo en la implementación de las iniciativas de la hoja de ruta del Plan de Ciberseguridad, el faltante de recurso humano, por lo que, en el Plan Reforzado de Ciberseguridad, se propuso la conformación del equipo de Ciberseguridad de la red integrada de servicios TIC, no obstante, el mismo no se ha materializado.

A nivel normativo, se evidenció que la normativa vigente en materia de Ciberseguridad y Seguridad de la Información no se ha actualizado, presentándose incluso Políticas y Normas que datan del 2007 y 2008, pese a la existencia de una iniciativa en la hoja de ruta del Plan de Ciberseguridad que busca su actualización y subsanar brechas existentes.

Se determinaron aspectos de mejora en torno a la coordinación del área de Seguridad y Calidad con el área de Ingeniería en Sistemas, lo anterior debido a que esta última identificó la necesidad de iniciar un proceso de contratación relacionado con software seguro, donde el objetivo principal es la incorporación de prácticas de desarrollo seguro en la fábrica de software y en los equipos de desarrollo, no obstante, el Plan de Ciberseguridad tiene en ejecución la iniciativa PCS-GI-16 denominada “Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software”.

Finalmente, se determinó que, si bien en el Plan de Ciberseguridad se llevó a cabo una identificación de riesgos, se evidenciaron oportunidades de mejora en el tratamiento de estos en torno a la medición, evaluación, control y seguimiento.

En virtud de lo expuesto, este Órgano de Fiscalización emitió conclusiones y recomendaciones, con la finalidad de que la Institución revise el Plan de Fortalecimiento de Ciberseguridad y analice el replanteamiento de la misma considerando los aspectos de mejora identificados en el presente estudio.

ATIC-0095-2023
4 de diciembre de 2023

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN Y CONTROL EN EL AVANCE DE LA IMPLEMENTACIÓN DE LAS INICIATIVAS DERIVADAS DEL PLAN DE CIBERSEGURIDAD

GERENCIA GENERAL-1100
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo 2023 para el Área de Auditoría de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión y el control que realiza la administración activa en torno al avance en la implementación de las iniciativas derivadas del Plan de Ciberseguridad.

OBJETIVOS ESPECÍFICOS

1. Identificar el cumplimiento de la normativa establecida a nivel de sector público e institucional en torno a gestión de proyectos en la ejecución del Plan de Ciberseguridad.
2. Comprobar el avance real en la implementación de las iniciativas definidas en la hoja de ruta del Plan de Ciberseguridad.
3. Verificar los mecanismos de control establecidos en la gestión de la implementación de las iniciativas de la hoja de ruta del Plan de Ciberseguridad.
4. Identificar la existencia del análisis de riesgos en la implementación de la hoja de ruta del Plan de Ciberseguridad.

ALCANCE

El estudio comprende la verificación de las acciones efectuadas por la Administración Activa en torno a la gestión de la implementación del Plan de Ciberseguridad, durante el periodo de enero de 2022 a setiembre de 2023, ampliándose en los casos que se estimó necesario.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público y Normas para el Ejercicio de la Auditoría Sector Público, divulgadas a través de la Resolución R-DC-064-2014 de la Contraloría General de la República, publicadas en La Gaceta 184 del 25 de setiembre 2014, vigentes a partir del 1º de enero 2015 y demás normativa aplicable.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Revisión y análisis de los documentos asociados al Proyecto CIBERTIC, específicamente el Plan de Ciberseguridad y su hoja de ruta.

- Verificación de la normativa institucional vigente, en torno a la gestión de proyectos, así como de Ciberseguridad y Seguridad de la Información.

- Verificación de la Agenda Digital Estratégica Institucional (AGEDI) y los informes de avance trimestrales del 2023 emitidos por la Dirección de Tecnologías de Información y Comunicaciones (DTIC)

- Revisión y análisis de las minutas de las sesiones del Consejo Tecnológico Institucional del periodo 2022-2023.

- Aplicación de entrevistas y análisis de información aportada por:

    - Máster Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática.
    - Ing. Erick Vindas Umaña, jefe de la subárea de Seguridad Informática.
    - Ing. Vanessa Carvajal Carmona, anterior jefatura de la subárea de Seguridad Informática.
    - Máster Danilo Hernández Monge, anterior subdirector de la Dirección de Tecnologías de Información y Comunicaciones con recargo del área de Seguridad y Calidad Informática.

- Solicitud de información al Máster Luis Diego Peña Ledezma, jefe de Subárea Administración de Proyectos, Ing. Vanessa Carvajal Carmona, jefe del área de Soporte Técnico y Máster Sergio Porras Solís, jefe del área de Comunicaciones y Redes Informáticas.

MARCO NORMATIVO

- Ley General de Control Interno 8292, agosto 2002.
- Normas de Control Interno para el Sector Público de la Contraloría General de la República, febrero 2009.
- Normas técnicas para la gestión y control de las tecnologías de información, MICITT, noviembre 2021.
- Normas Institucionales en Tecnologías de Información y Comunicaciones, abril 2012.
- Manual funcional del Consejo Tecnológico Institucional, octubre 2020.
- Manual de la Agenda Digital Estratégica Institucional, enero 2022.
- Directriz para la gobernanza de TIC GG-DTIC-EDM01-IT002, setiembre 2020.
- Ficha del proceso APO05 – Gestionar el portafolio, setiembre 2020.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)"*

ANTECEDENTES

El 5 de marzo de 2019 el Ing. Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones e Ignacio Pérez Rubio, Apoderado Generalísimo sin límite de suma de la empresa Price Waterhouse Coopers Consultores, S.R.L, formalizaron el contrato n° 004-2019, derivado de la Licitación Abreviada N° 2019LA-000001-1150, cuyo objeto era: "Servicios Profesionales para desarrollar Plan de Ciberseguridad para la CCSS".

El 26 de abril 2019 se presenta la versión inicial del plan que establecía como objetivos los siguientes:

> *"2.1. Objetivo general*
>
> *Desarrollar un plan de Ciberseguridad en la CCSS, el cual cuente con los aspectos necesarios para una adecuada estrategia de seguridad de las TIC.*
>
> *2.2. Objetivos específicos*
>
> *Para el desarrollo del proyecto se han establecido los siguientes objetivos específicos, que corresponden con las fases establecidas para la contratación:*
>
> *• Identificar y documentar la situación actual de la seguridad en TIC de la CCSS, tomando en cuenta las localidades definidas en el alcance*
> *• Diseñar el Plan de Ciberseguridad para la CCSS considerando elementos deseados y tendencias, alineado con la normativa aplicable para la CCSS y el Modelo meta de gobernanza y gestión de TIC y Seguridad de la Información.*
> *• Identificar las brechas con base en la normativa vigente aplicable a la CCSS y los estándares internacionales.*
> *• Documentar la hoja de ruta de implementación de las brechas identificadas para cumplir con el Plan de Ciberseguridad para la CCSS, así como las acciones de gestión de cambio a futuro.*
> *• Diseñar y documentar 10 de las iniciativas identificadas en la hoja de ruta.*
> *• Utilizar 1000 horas en un periodo de 12 meses para realizar actividades aprobadas en la fase de Hoja de ruta en las siguientes actividades:*
>
> *o Actividades relacionadas a la gestión de cambio.*
> *o Diseño y desarrollo de estudios adicionales de acuerdo a la hoja de ruta".*

Además, en cuanto a las fases y entregables, se estableció:

> *"Esta consultoría se ejecuta en 7 fases; las primeras 5 buscan desarrollar el Plan de Ciberseguridad para la CCSS. Por otra parte, la sexta fase corresponde al diseño y documentación de 10 iniciativas iniciales definidas en la hoja de ruta, por último, la fase 7 corresponde al uso de horas contra demanda para la ejecución de actividades enfocadas en la implementación del Plan de ciberseguridad La siguiente tabla ofrece una vista resumen de las fases y entregables de la consultoría…".*

Plan de Ciberseguridad: hoja de ruta y priorización de iniciativas

El 28 de mayo de 2020, se firmó el acta de recepción definitiva del Informe de Análisis de situación actual de la seguridad en TIC, así como el Informe de resultado del análisis de vulnerabilidades técnicas por parte del equipo de proyecto designado por la Dirección de Tecnologías de Información y Comunicaciones. Por lo anterior, el 15 de junio de 2020, mediante oficio GG-DTIC-3409-2020, el Máster Manuel Montillano Vivas, administrador del contrato No. 004-2019 de la Licitación Abreviada No. 2019LA-000001-1150, le entregó al Máster Robert Picado Mora, el producto de la fase dos del proyecto de Ciberseguridad relacionado con la identificación, definición y documentación de la situación actual de la seguridad en TIC de la CCSS.

El 15 de diciembre 2020 se aprobó por parte de Isaac Rodríguez Rojas, director de proyecto de la empresa contratada Price Waterhouse Cooper, y de Manuel Montillano Vivas, director de proyecto por parte de la CCSS, el documento PCS-ENT-029 "Plan de Ciberseguridad" el cual especificaba 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 las brechas de ciberseguridad detectadas a nivel Institucional, lo anterior de conformidad con la aplicación de un esquema de puntaje, así como el análisis y estado actual de la CCSS realizado en las fases No. 2 y No. 4 de la contratación.

El 28 de setiembre de 2021 mediante oficio GG-DTIC-5735-2021, el Máster Roberto Blanco Topping, Sub-Gerente a.i. de la Dirección de Tecnologías de Información y Comunicaciones, conformó el equipo de trabajo para la implementación de las 23 iniciativas del Plan de Ciberseguridad las cuales fueron establecidas dentro del Modelo Meta de Gobernanza y Gestión de las TIC, denominado "Servicios Profesionales para desarrollar un Plan de Ciberseguridad para la Caja Costarricense de Seguro Social", Licitación Abreviada 2019LA-000001-1150, dicho equipo de trabajo quedó conformado por el Máster Christian Chacón Rodríguez, Subdirector de la Dirección de Tecnologías de Información y Comunicaciones en ese momento, la Máster Mayra Ulate Rodríguez, jefe del área de Seguridad y Calidad Informática, la Licda. Vanessa Carvajal Carmona, jefe a.i. de la Subárea de Seguridad en Tecnologías de Información y la Máster Ericka Sánchez Solís funcionaria de la Subárea de Seguridad en Tecnologías de Información.

Sobre las 23 iniciativas de la hoja de ruta del Plan de Ciberseguridad

El documento "PCS-ENT-29 Plan de Ciberseguridad", define 23 fichas de proyectos, que una vez implementados permitirían que las brechas entre el estado actual y el estado objetivo deseado puedan subsanarse y fomentar una robusta gestión de la ciberseguridad en la Caja Costarricense de Seguro Social.

Las 23 iniciativas son los siguientes:

Cuadro N° 1
Iniciativas que integran la hoja de ruta del Plan de Ciberseguridad
Diciembre 2020

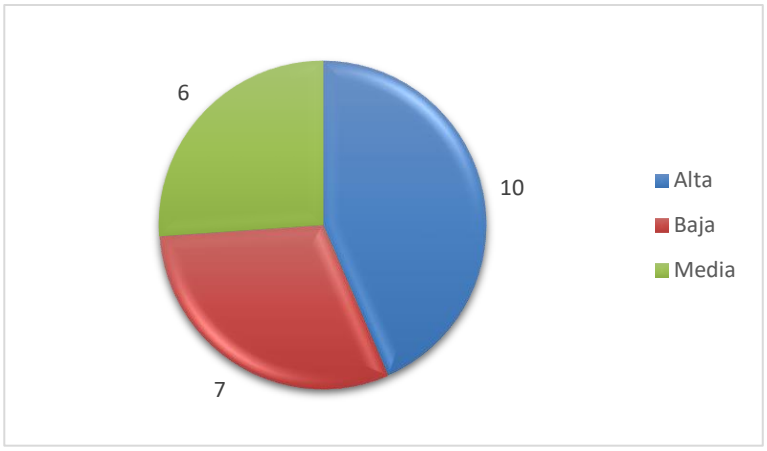
	# Iniciativa	Descripción Iniciativa
1	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.
2	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.
3	PCS-GI-03	Iniciativas 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
4	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.
5	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.
6	PCS-GI-06	Iniciativas para el desarrollo de una estrategia de respaldos institucional
7	PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético.
8	PCS-GI-08	Iniciativas para la definición de una arquitectura de ciberseguridad que se alinee con los objetivos de la DTIC.
9	PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.
10	PCS-GI-10	Iniciativas para implementar el Plan de Concientización en Ciberseguridad.
11	PCS-GI-11	Iniciativas para la implementación de la gestión de la seguridad de los endpoint.
12	PCS-GI-12	Iniciativas para el fortalecimiento de la identidad y gestión de acceso.
13	PCS-GI-13	Iniciativas para la gestión del acceso privilegiado en los sistemas de la CCSS
14	PCS-GI-14	Iniciativas para el establecimiento e implementación de las líneas base de seguridad.
15	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.
16	PCS-GI-16	Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software.
17	PCS-GI-17	Iniciativas para la simulación de ataques y pruebas de seguridad
18	PCS-GI-18	Iniciativas para la implementación de la gestión de la seguridad en la nube.
19	PCS-GI-19	Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.

20	PCS-GI-20	Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.
21	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.
22	PCS-GI-22	Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC.
23	PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral

Fuente: Documento PCS-ENT-29 Plan de Ciberseguridad

En dichas fichas se establecieron aspectos como plazos estimados de ejecución de la iniciativa, etapa de implementación y prioridad, mismos que actualmente se identifican de la siguiente forma:

Gráfico N° 1
Cantidad de iniciativas según prioridad
Plan de Ciberseguridad
Diciembre de 2020

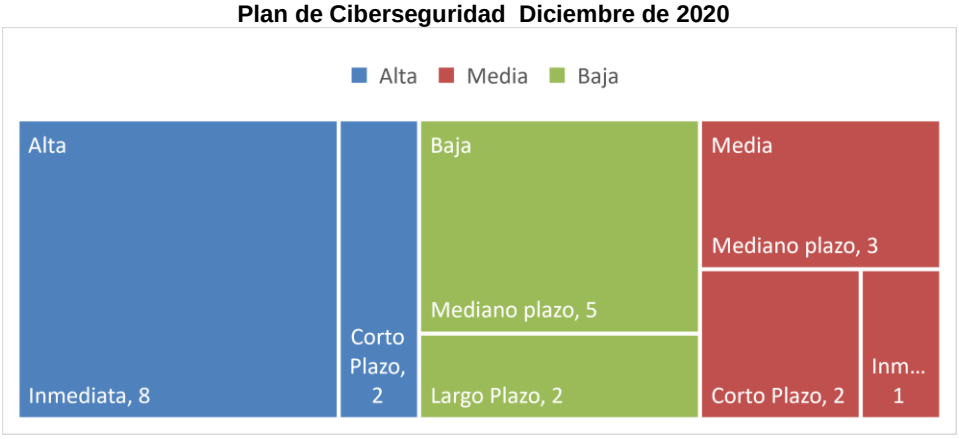


Fuente: Documento PCS-ENT-29 Plan de Ciberseguridad

En el gráfico 1 se observa que, de las 23 iniciativas planteadas, 10 tienen una prioridad alta, 6 media y 7 baja.

Asimismo, al analizar la etapa de implementación de cada una de ellas se identifica lo siguiente:

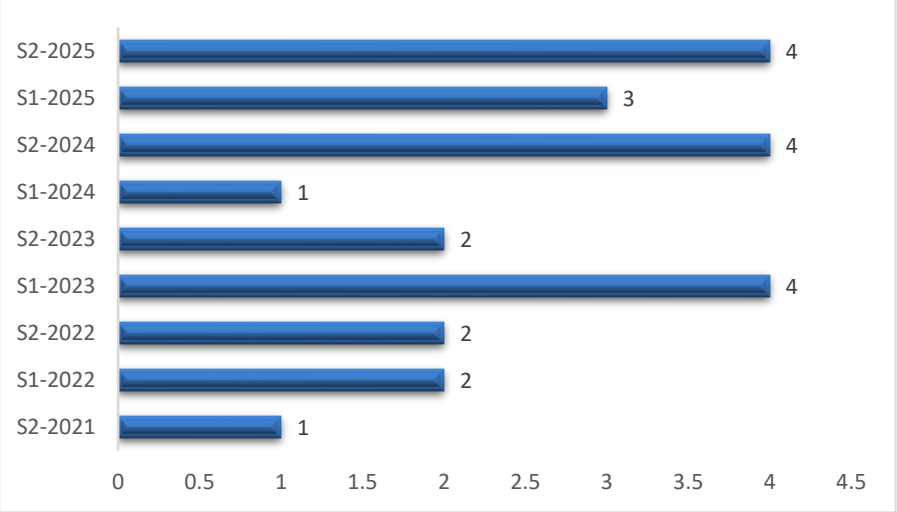
Gráfico N° 2
Cantidad de iniciativas según prioridad y etapa de implementación
Plan de Ciberseguridad Diciembre de 2020



Fuente: Documento PCS-ENT-29 Plan de Ciberseguridad

En el gráfico anterior, se observa las etapas de implementación de cada una de las 23 iniciativas a saber, atención inmediata, corto plazo, mediano plazo y largo plazo, identificándose además que están distribuidas para realizarse del II semestre del 2021 al II semestre del 2025 según el siguiente detalle:

Gráfico N° 3
Cantidad de iniciativas según plazo estimado de ejecución
Plan de Ciberseguridad
Agosto de 2022



Fuente: Oficio GG-DTIC-4325-2022

Respecto a la propuesta de fortalecimiento del Plan de Ciberseguridad

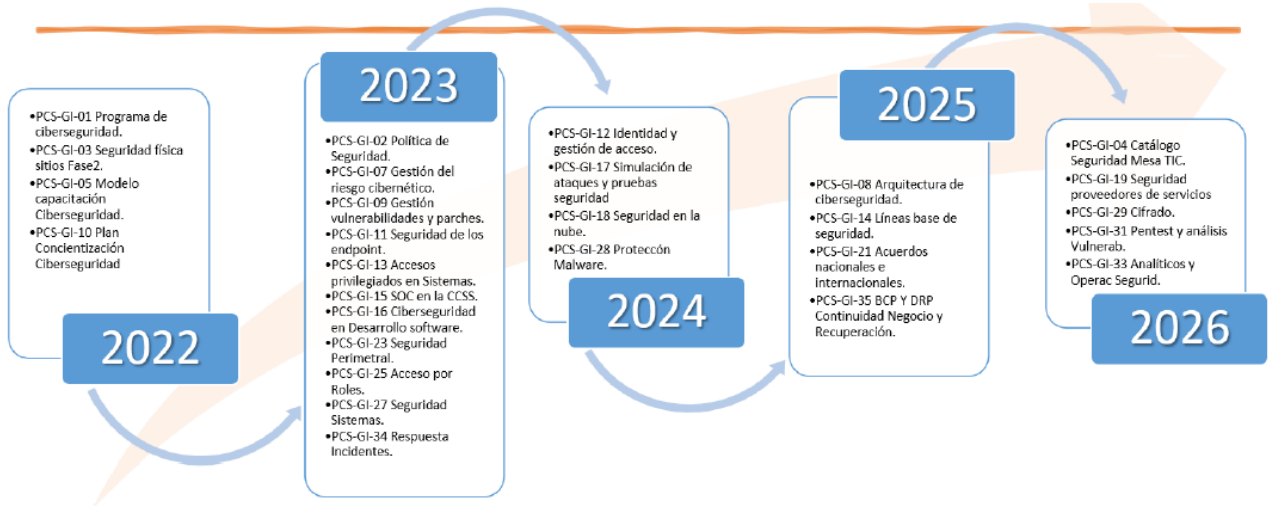
Producto del ataque informático que recibió la CCSS el 31 de mayo de 2022, la Dirección de Tecnologías de Información y Comunicaciones con el apoyo de diversos proveedores como Deloitte, Microsoft, GBM, así como entes asesores, tales como: el Centro Criptológico Nacional Español (CN-CERT), el Ministerio 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 deben ser incorporados en los esfuerzos que la Institución venía realizando en materia de ciberseguridad.

Por lo anterior, la DTIC elaboró una actualización del Programa denominado: “Fortalecimiento del Plan de Ciberseguridad”, el cual contempla 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 es presentar una propuesta de abordaje que cubra 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.

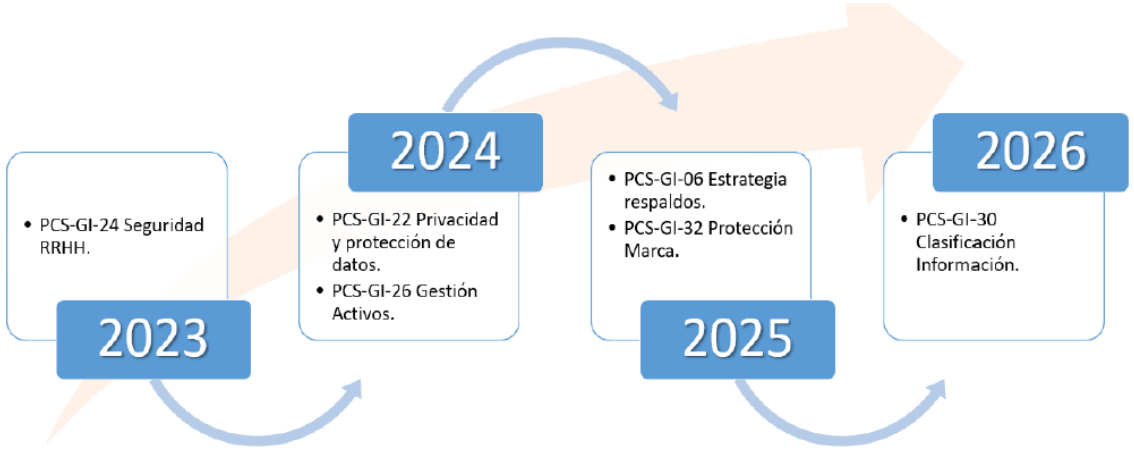
La estrategia planteada constituye un compendio de iniciativas propuestas en un marco de abordaje integral, que permite en su conjunto atender una serie de acciones requeridas para reforzar la seguridad cibernética. Este conjunto de iniciativas corresponde a 34 propuestas, de las cuales 28 responde a acciones de ciberseguridad, en tanto 6 a seguridad de la información, según el siguiente detalle:

Gráfico N° 4
Iniciativas con enfoque de ciberseguridad y su línea de tiempo
Plan de Fortalecimiento Proyecto Ciberseguridad
Noviembre de 2022



Fuente: Documento "Plan de Fortalecimiento Proyecto Ciberseguridad"

Gráfico N° 5
Iniciativas con enfoque de seguridad de la información y su línea de tiempo
Plan de Fortalecimiento Proyecto Ciberseguridad
Noviembre de 2022



Fuente: Documento "Plan de Fortalecimiento Proyecto Ciberseguridad"

Costo estimado de la implementación de las iniciativas de la hoja de ruta del Plan de Ciberseguridad

El 20 de febrero de 2023 mediante oficio GG-DTIC-0932-2023, los ingenieros Ericka Sánchez Solís, jefe a.i. de la Subárea de Seguridad Informática, Luis Diego Peña Ledezma, jefe subárea Administración de Proyectos, Adriana Moreira Madrigal, analista de la Subárea de Administración de Proyectos, Esteban Zamora Chaves, asistente de despacho, y Danilo Hernández Monge, subdirector a.i. todos de la Dirección de Tecnologías de Información y Comunicaciones, le informaron al Máster Eithel Corea Baltodano, Sub Gerente de la DTIC, sobre aspectos comentados en la sesión del Consejo Tecnológico en el que se presentó el Plan Fortalecido de Ciberseguridad, donde en el apartado "I. Sobre costos iniciales estimados al desarrollo de las iniciativas del Programa" indica:

"Por lo anteriormente detallado, y bajo el entendido de que las iniciativas de ciberseguridad son las que estará desarrollando en su totalidad la DTIC, se contempló en la propuesta original planteada como parte del proyecto de diseño e implementación de un Modelo Meta de Gobierno de Tecnologías de Información y Comunicaciones y Gobierno de la Seguridad de la Información, una definición preliminar de costos correspondiente al desarrollo de las iniciativas ya definidas con referencia al recurso humano y los insumos que se deben adquirir para el cumplimiento de cada una de ellas, como lo son hardware, licenciamiento, entre otros. Los costos estimados de las iniciativas a desarrollar en el 2023 corresponden a:

Tabla N°3

Costos de las iniciativas año 2023

Código	Descripción	Costo estimado por iniciativa de este monto se encuentra los costos por adquisición de tecnologías y los costos de Recurso Humano).
PCS-P-02	Desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes	₡222.124.996,80
PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético	₡28.390.000,00
PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.	₡124.348.200,00
PCS-GI-11	Iniciativas para la implementación de la gestión de la seguridad de los endpoint	₡489.727.500,00
PCS-GI-13	Iniciativas para la gestión del acceso privilegiado en los sistemas de la CCSS.	₡57.489.750,00
PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS	₡4.033.970.508,01
PCS-GI-22	Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC.	₡170.907.800,00
PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral	₡846.022.000,00
PCS-GI-25	Iniciativas de acceso por roles.	₡222.124.996,80
PCS-GI-27	Iniciativas a nivel de Seguridad Sistemas	₡222.124.996,80
PCS-GI-34	Respuesta a Incidentes	₡222.124.996,80
	TOTAL	₡6.639.355.745,21

„

Productos emitidos por la Auditoría Interna

La Auditoría Interna ha emitido en los últimos 3 años, productos relacionados con el Proyecto CIBERTIC, así como del Plan de Ciberseguridad y su hoja de ruta, donde se han identificado aspectos de mejora en torno a la gestión integral del proyecto "Plan de Ciberseguridad de la CCSS", asimismo, a la gestión de Gobierno y de Ciberseguridad donde se determinó la ausencia de un modelo de gobierno de la seguridad informática a nivel institucional y la ausencia de una estrategia integral de ciberseguridad, además lo referido a materia de roles y responsabilidades de ciberseguridad en la CCSS. (ver anexo 1)

HALLAZGOS

1. SOBRE LA GESTIÓN DEL PLAN DE CIBERSEGURIDAD Y SU HOJA DE RUTA CON PERSPECTIVA DE PROYECTOS

Se identificó que la ejecución de la hoja de ruta del Plan de Ciberseguridad no es gestionada como un proyecto o programa de proyectos, donde se definan actividades que valoren aspectos de alcance, tiempo, presupuesto y uso óptimo de los recursos, así como que se realice la medición del desempeño, e identificación de mejora, lo anterior mediante el uso de indicadores que permitan controlar el nivel del logro de las metas planteadas.

Si bien para cada una de las 23 iniciativas se diseñó una ficha técnica que considera aspectos como: etapa de implementación, alcance, objetivo, prioridad, plazo de ejecución estimado, costo estimado, riesgos asociados, roles responsables e indicadores los cuales describen las métricas identificadas para la medición y evaluación de los resultados de la ejecución del proyecto o grupo de iniciativas, en los informes presentados del avance de la ejecución de las iniciativas no se observa la utilización de dichos indicadores definidos para el análisis correspondiente del avance en la ejecución de la hoja de ruta.

Asimismo, considerando los procesos básicos de la metodología de proyectos se identificó lo siguiente:

ALCANCE: El Plan de Ciberseguridad propiamente, tiene definido su alcance en las 6 fases descritas anteriormente: Planificación, Análisis Actual, Diseño del estado deseado, Brechas, hoja de ruta y mejoras prioritarias. Respecto a la hoja de ruta se tienen definido las 23 iniciativas que atienden las brechas identificadas en las fases 2 y 4, no obstante, debido al ciberataque sufrido el 31 de mayo de 2022, se presentó en noviembre de 2022 la propuesta del “Plan Reforzado de Ciberseguridad” en el cual se contempla ampliar a un total de 35 iniciativas.

TIEMPO: Los tiempos identificados en el Plan de Ciberseguridad fueron definidos por plazos de ejecución con el siguiente detalle:

- Corto plazo: Con un plazo de implementación de 1 a 3 años.
- Mediano plazo: Con un plazo de implementación de 3 a 5 años.
- Largo plazo: Con un plazo de implementación mayor a 5 años.

Una vez que se contó con la lista definitiva de iniciativas a implementar, las mismas se colocaron en la hoja de ruta a un plazo de los 5 años de la estrategia, la cual tendría revisiones y ajustes anuales de acuerdo con las necesidades identificadas en la Caja Costarricense de Seguro Social.

Sin embargo, no se identificó en la hoja de ruta ni en la información aportada por la Administración, que se estableciera un cronograma con las tareas de cada iniciativa, pese a que en estas se definieron las actividades a llevar a cabo para la implementación de cada una de ellas, por lo que no se lleva el control mediante el avance del cumplimiento por tareas.

COSTO: se identificaron los tipos de recursos necesarios para llevar a cabo el grupo de iniciativas, los cuales fueron dimensionados según su clasificación, a saber: costos internos, soluciones tecnológicas, infraestructura tecnológica, servicios de consultoría, servicios de capacitación, en la ficha se describe el costo estimado no obstante en los informes periódicos no se observa que se le brinde seguimiento a este indicador.

El Plan de Ciberseguridad PCS-ENT-029, en el apartado 4 “Objetivo”, señala:

> *“El objetivo de este informe es documentar la hoja de ruta para la implementación del Plan de Ciberseguridad en la Caja Costarricense de Seguro Social* ***por medio de proyectos e iniciativas priorizadas*** *de acuerdo con los riesgos de seguridad de las TIC, necesidades que posee la Institución actualmente y el estado objetivo deseado.*

Adicionalmente, para cada proyecto e iniciativa mencionada en la hoja de ruta se puede visualizar las interdependencias con otros proyectos, costos y plazos estimados para su implementación". (la negrita no es del original)

Asimismo, en el apartado 6.6 "Etapa 6: Hoja de ruta" se indica:

"Durante esta etapa se documentó en una hoja de ruta ***los proyectos o grupo de iniciativas priorizadas*** *que se deben llevar a cabo en un período de 5 años con el objetivo de implementar el presente plan y reforzar la gestión de la ciberseguridad en la Caja Costarricense de Seguro Social, la cual permita cerrar la brecha existente entre el estado actual y el estado deseado objetivo que se definió en la fase 3 – Diseño del estado deseado".*

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002, en su apartado 8.11 establece:

"8.11 Todo proyecto e inversión en TIC deberá ser controlada, con el fin de conocer el rendimiento en la ejecución de los gastos, los beneficios obtenidos y los costos asociados*.*

Es necesario controlar el rendimiento en términos económicos de las inversiones de TIC con el fin de apoyar el cumplimiento de la normativa asociada al control interno y gestión de las finanzas públicas, así como generar información histórica que permita mejorar los procesos de formulación, y asegurar el aprovechamiento de los recursos públicos.

8.11.1 Mecanismos

Se definirán métricas básicas de desempeño para los proyectos e inversiones en TIC, aunado a esto se desarrollarán y vigilará el cumplimiento de normativa para el control del gasto, costos y presupuesto asociados a través de informes de medición periódicos, generados a través del proceso APO05 – Gestionar el portafolio. Se remitirá un reporte trimestral al Consejo Tecnológico sobre el desempeño y estado actual del portafolio de proyectos e inversiones en TIC". (la negrita no es del original)

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en el punto "IX. Gestión de Proyectos que Implementan Recursos Tecnológicos" detallan:

"La institución debe gestionar los proyectos que permitan habilitar sus iniciativas para el logro de los objetivos estratégicos, satisfaciendo los requerimientos y en cumplimiento con ***términos de calidad, tiempo, presupuesto y uso óptimo de los recursos****, de acuerdo con las buenas prácticas y estándares preestablecidos.*

La Unidad de TI debe establecer el portafolio de proyectos debidamente priorizados, identificando en cada iniciativa el beneficio a generar por la habilitación de tecnologías de información. Su administración ***a través de la ejecución de los planes asociados, deben permitir obtener el resultado esperado, minimizando el riesgo asociado a eventos durante la ejecución del proyecto*** *y garantizando la calidad y la entrega de valor para el logro de los objetivos institucionales.*

La Unidad de TI debe establecer un modelo estandarizado para la gestión y administración de proyectos de perfil tecnológico, así como su continua actualización, divulgación y capacitación a funcionarios". (la negrita no es del original)

Asimismo, en la descripción del Perfil del Proceso, la misma norma indica:

"*PERFIL DEL PROCESO*

Para asegurar que se realiza una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, debe asegurarse que cumpla con el siguiente perfil:

1. *Debe estar formalmente definido a través de la disposición de un objetivo claro y metas específicas, que sean ejecutables, reales, orientadas a resultados y medibles.*

*2. La propiedad del proceso debe estar claramente establecida, sobre el diseño, interacción con otros procesos**, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora**.*

*3. **Debe estar claramente establecida la secuencia de actividades de forma lógica, consecuente, flexible, y escalable de forma tal que produzca los resultados esperados**, considerando el manejo de excepciones y emergencias.*

4. Los roles y responsabilidades deben estar exactamente asignados para la ejecución efectiva de las actividades clave y su documentación, además de la rendición de cuentas sobre los entregables finales asociados.

5. Debe disponer de lineamientos y planes debidamente formalizados, revisados, actualizados, aprobados, almacenados, comunicados, publicados y utilizados en forma consecuente, que establezcan las directrices y acciones requeridas. Los lineamientos deben estar accesibles y asegurar el claro entendimiento por parte de los responsables de su aplicación, así como de las partes interesadas. (…)

*6. **Deben contar con indicadores de desempeño, de tal forma que permitan identificar el nivel de logro de las metas**. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique". (la negrita no es del original)*

El Máster Danilo Hernández Monge, subdirector a.i. de la DTIC, el 8 de noviembre de 2022 mediante oficio GG-DTIC-6407-2022, remitido a esta Auditoría, respecto a la implementación del Plan de Ciberseguridad indicó:

"En ese sentido, más allá de la necesidad de fortalecer las capacidades de recurso humano en el Área y aprovechando el esfuerzo de fortalecimiento del plan de ciberseguridad, se está trabajando en replantear el enfoque de gestión del Plan de Ciberseguridad bajo el modelo de "PROGRAMA", alineado a los procesos de la Agenda Digital (AGEDI), en procura de promover la atención del plan de forma diferente, lo cual implica especificar iniciativas y la gestión que permita transformarlas en proyectos y que este proceso, ayude a identificar y asegurar los recursos que cada proyecto requiere, evidenciando los requisitos asociados y el aseguramiento de condiciones para que cada iniciativa sea gestionada".

Mediante oficio GG-DTIC-3964-2022 del 18 de agosto de 2022, el Máster Danilo Hernández, subdirector a.i. de la DTIC y la Máster Vanessa Carvajal Carmona, jefe de la subárea de Seguridad Informática en ese momento, le informan a la Máster Idannia Mata Serrano, Sub-Gerente a.i. de la DTIC lo siguiente:

"Como parte de las labores realizadas en la Dirección de Tecnologías, se han planificados los presupuestos para el periodo comprendido entre 2021 y 2025 ya se encuentran contemplados los costos para dar cumplimiento al Plan de Ciberseguridad, el cual busca tener cubierto las 23 iniciativas".

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informáticas, señalaron a esa auditoria lo siguiente:

"(…) sobre este tema existe una deuda, porque realmente se tenía que dar un control de avance, sin embargo como parte del análisis para hacer la gestión de métricas, resultó este oficio 3443, sin embargo se está en ese proceso de retomar la parametrización de actividades para llegar y definir esto, Don Daniel ya tomó parte en el asunto, yo el pasado 29 de agosto mandé un oficio a los sub alternos, delegando responsabilidades entre estos temas, establecer el control de avance, y se estableció plazo al próximo 29 de setiembre para la presentación de este tema en concreto.

Hay tareas que como tal y como se recibió el mismo proyecto, no existe una parametrización correcta, donde por ejemplo para la iniciativa 23 que habla de seguridad perimetral, aunque estamos llevando un proceso de implementación de esta tecnología que ya está en fase 2, no hay una parametrización correcta para indicar cuando porcentaje de avance se tiene, realmente sobre este tema se está generando este informe con actualización de métricas como tal, estuve hablando con Alonso Madrigal a quién se le delegó esta tarea y se le dijo que entre las tareas que puede ir avanzando son la 9 y 14 que son las que se tienen bajo contrato, de igual manera se están dando insumos para que él vaya actualizando, porque por ejemplo a febrero de este año, la iniciativa 2 que es sobre normativa, esta está hecha, se trasladó a la Dirección, para que hiciera el proceso de aprobación y publicación, pero se quedó pegada en la Dirección de igual manera tenemos avances significativos en la 5 y la 10 que hablan sobre la concientización y marco de capacitación en Ciberseguridad, en el cual ustedes ya han sido testigos de los cursos que se han enviado por Web Master en alianza con MICIIT y la fundación Omar Dengo pero que por no tener métodos de parametrización no se han podido incorporar a este modelo de gestión de avance, pero si estamos trabajando en esto.

Se va a hacer el esfuerzo necesario para que al 29 de setiembre, se tenga un Dashboard para que se refleje el avance de cada una de las iniciativas que se han venido desarrollando, casualmente la compañera que recientemente ingresó a la subárea maneja el tema de DashBoard y ya le solicitamos la colaboración, se está reuniendo la información para poderlo tabular y ya tenerlo con cada una de las iniciativas".

Lo identificado en cuanto a la ausencia de gestión desde una perspectiva de proyectos o programa de proyectos de la hoja de ruta del Plan de Ciberseguridad, conlleva al debilitamiento del control sobre aspectos críticos como el alcance, el tiempo y el costo. Aumentando no solo el riesgo de desviaciones en la implementación de cada una de las iniciativas definidas, sino que también dificulta la evaluación precisa de los recursos necesarios y los plazos de entrega. La carencia de esta metodología compromete la eficiencia y eficacia en la protección de activos digitales, exponiendo potencialmente a la organización a mayores vulnerabilidades y amenazas de seguridad.

2. SOBRE LA INCLUSIÓN DEL PLAN DE CIBERSEGURIDAD AL AGEDI

Se identificó que el Plan de Ciberseguridad vigente se encuentra integrado al AGEDI como mecanismo de control y seguimiento del proyecto, no obstante, este se incluyó en la Agenda con el alcance orientado a la definición de dicho plan, por lo que al estar formalizado el entregable, este proyecto aparece actualmente con un nivel de cumplimiento del 100%, quedando pendiente la inclusión de la hoja de ruta, donde se pueda controlar la implementación de las iniciativas y su avance correspondiente en aquellas que deban estar incluidas en dicha agenda.

Al respecto en el informe trimestral correspondiente al II trimestre del 2023 del AGEDI, este indica:

*"**6. Establecer el Plan de Ciberseguridad en TIC institucional***

El Proyecto de Ciberseguridad en TIC Institucional inició el 27 de marzo de 2019. El principal beneficio de este proyecto es el diseño de un plan de Ciberseguridad en la CCSS, el cual cuente con los aspectos necesarios para una adecuada estrategia de seguridad de las TIC.

El proyecto de Ciberseguridad en TIC muestra un avance de un 100% en la ejecución del plan de Ciberseguridad, con una inversión a la fecha de $329.000,00 (¢200.4 millones de colones)"

Sobre esto, el mismo Plan de Ciberseguridad PCS-ENT-029, en el apartado de identificación de los plazos estimados indica:

> *"Adicionalmente, se contempló el período requerido para la documentación de los requisitos solicitados por la AGEDI**, a fin de formalizar los grupos de iniciativas como proyectos**. Asimismo, se contemplaron los plazos de contratación administrativa, de acuerdo con la información remitida por el AGEDI (…).*
>
> *En este sentido, el plazo estimado que se muestra dentro de la ficha de cada proyecto o grupo de iniciativas se compone por:*
>
> *• Cantidad de meses requeridos para la documentación y aprobación del proyecto ante el AGEDI*
> *• Cantidad de meses necesarios según el tipo de contratación administrativa*
> *• Cantidad de meses que toma planificar, desarrollar e implementar el proyecto.*
>
> *Por otra parte, se debe considerar que no todos los proyectos o grupos de iniciativas requieren aplicar el proceso de contratación administrativa ya que pueden ser ejecutados completamente con recursos internos, por lo tanto, en estos casos solo se contempla el **plazo de inclusión del proyecto en la AGEDI** y el de su planificación, desarrollo e implementación.*
>
> *Otro punto para tomar en cuenta es que las iniciativas que componen cada ficha podrán ser ejecutadas por etapas debido a la complejidad de implementación de cada grupo de iniciativas. Sin embargo, esto no significa que cada etapa es independiente de la otra, ya que los productos finales de unas serán utilizados como insumos para las etapas posteriores. Por ejemplo, el grupo de iniciativas PCS-GI-15, que corresponde a las iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS, se divide en tres etapas: diseño, operación e implementación; cada una tiene un nivel elevado de complejidad, por lo tanto, ante el AGEDI, cada etapa se podrá visualizar como un proyecto separado el cual tendrá diferentes plazos". (La negrita no es del original)*

Asimismo, en el punto 6.5 "Etapa 5. Brechas para alcanzar el estado deseado" se explica lo que contiene cada ficha de cada iniciativa, especificando para el Grupo de Iniciativas o proyecto lo siguiente:

> *"Dentro de la ficha solo es requerido definir el nombre que se le otorga a dicho grupo de iniciativas. Cabe destacar que cada grupo de iniciativas podrá convertirse en un proyecto, una vez cumplidos los requisitos de la AGEDI"*

El Manual de la Agenda Digital Estratégica Institucional en su apartado 5 "Agenda Digital Estratégica Institucional señala:

> *"La AGEDI registra información clave de los programas y proyectos para facilitar la toma de decisiones y el seguimiento, cuya fuente de información se encuentra en los documentos, reportes y mecanismos que se han definido como el medio de retroalimentación y estado de los proyectos. Así, por ejemplo, en la AGEDI se incluye una referencia o resumen de los riesgos de un programa o proyecto, mientras que la identificación y la valoración de riesgos y las estrategias para su gestión estarán en los casos de negocio u otros documentos de seguimiento y gestión.*
>
> *Por otra parte, la AGEDI permite la generación de información necesaria para apoyar el análisis y gestión de portafolio; por ejemplo, elementos para identificar los impactos esperados en los servicios TIC o en el modelo operativo institucional".*

La Directriz para la Gobernanza de TIC en su punto 8.5 indica:

> *"La Agenda Digital Institucional constituye el portafolio integral e institucional de proyectos e inversiones con componente TIC, esto permite una adecuada coordinación de los recursos requeridos para su desarrollo, al tiempo que aporta visibilidad de los esfuerzos que la CCSS está realizando en transformación y operación de servicios TIC. Por lo anterior, se asignarán recursos para su desarrollo únicamente a aquellos proyectos que hayan sido valorados y aprobados conforme a las disposiciones y procedimientos establecidos en la presente directriz y en los procesos Banco de Iniciativas y Portafolio de Proyectos TIC (específicamente en lo que se refiere a proyectos con componente TIC)".*

El Máster Danilo Hernández Monge, subdirector a.i. de la DTIC, el 8 de noviembre de 2022 mediante oficio GG-DTIC-6407-2022, dirigido a esta Auditoría, respecto a la implementación del Plan de Ciberseguridad indicó:

> *"En ese sentido, más allá de la necesidad de fortalecer las capacidades de recurso humano en el Área y aprovechando el esfuerzo de fortalecimiento del plan de ciberseguridad, se está trabajando en replantear el enfoque de gestión del Plan de Ciberseguridad bajo el modelo de "PROGRAMA", alineado a los procesos de la Agenda Digital (AGEDI), en procura de promover la atención del plan de forma diferente, lo cual implica especificar iniciativas y la gestión que permita transformarlas en proyectos y que este proceso, ayude a identificar y asegurar los recursos que cada proyecto requiere, evidenciando los requisitos asociados y el aseguramiento de condiciones para que cada iniciativa sea gestionada".*

El 20 de febrero de 2023 mediante oficio GG-DTIC-0932-2023, los ingenieros Ericka Sánchez Solís, jefe a.i. de la Subárea de Seguridad Informática, Luis Diego Peña Ledezma, jefe subárea Administración de Proyectos, Adriana Moreira Madrigal, analista de la Subárea de Administración de Proyectos, Esteban Zamora Chaves, asistente de despacho, y Danilo Hernández Monge, subdirector a.i. todos de la Dirección de Tecnologías de Información y Comunicaciones, le informaron al Máster Eithel Corea Baltodano, Sub Gerente de la DTIC, sobre aspectos comentados en la sesión del Consejo Tecnológico en el que se presentó el Plan Fortalecido de Ciberseguridad, donde en el apartado I "Sobre la gestión del plan de Ciberseguridad fortalecido bajo la figura de Programa" indicaron:

> *"La AGEDI es un mecanismo que apoya la gobernanza de las TIC, resumiendo información para apoyar la toma de decisiones sobre el portafolio institucional de programas y proyectos con componentes tecnológico.*
>
> *Este mecanismo mantiene una vista integrada y que se gestiona de forma continua, con inclusiones, modificaciones o eliminaciones en cualquier momento, y que permite generar ediciones o revisiones periódicas (semestrales, anuales, …) para enriquecer ciclos de gestión relacionados con estrategia y presupuestos, por ejemplo".*
>
> *De esta forma, el* ***Programa de Ciberseguridad y Seguridad de la información*** *se incorpora como tal en la AGEDI, para su seguimiento y gestión"*

No obstante, como se mencionó, dicho programa no se encuentra en el AGEDI según la revisión efectuada al informe del II trimestre del 2023.

La ausencia en el AGEDI de las iniciativas de la hoja de ruta del Plan de Ciberseguridad que deben tener un tratamiento de proyectos podría impedir un control efectivo y una supervisión integral de la implementación de cada una de ellas, dificultando la asignación adecuada de recursos, la definición de prioridades y la alineación con los objetivos generales de la Institución, lo que potencialmente expone a la CCSS a riesgos de seguridad cibernética no controlados y amenazas no mitigadas.

3. RESPECTO AL AVANCE DE LAS 23 INICIATIVAS DEL PLAN DE CIBERSEGURIDAD ORIGINAL

Se identificó el incumplimiento en la implementación de las iniciativas de la hoja ruta del Plan de Ciberseguridad cuyo plazo estimado de ejecución estaba definido para su finalización en el 2021, 2022 y 2023 respectivamente, asimismo se observó la atención de otra iniciativa que por el contrario estaba contemplada para el I Semestre del 2025 según se detalla:

El 31 de octubre de 2023 mediante oficio GG-DTIC-7306-2023, los Ingenieros Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad y Erick Vindas Umaña, jefe de subárea presentaron al Máster Robert Picado Mora, Sub-Gerente de la DTIC el informe trimestral del estado actual de las 23 iniciativas del Plan Táctico de Ciberseguridad para la Caja Costarricense de Seguro Social, en el cual se registra el siguiente nivel de avance:

Cuadro N° 2
Porcentaje de avance en la implementación de las 23
Iniciativas que integran la hoja de ruta del Plan de Ciberseguridad
31 de octubre 2023

	# Iniciativa	Descripción Iniciativa	Etapa implementación	Prioridad	Plazo estimado	T. Estimado	% Avance octubre 2023
1	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.	Inmediata	Alta	10 meses	S2-2021	100%
2	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Inmediata	Alta	6 meses	S2-2022	100%
3	PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral	Inmediata	Alta	15 meses	S1-2023	100%
4	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Inmediata	Alta	38 meses	S2-2023	100%
5	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.	Mediano plazo	Baja	6 meses	S1-2025	100%
6	PCS-GI-10	Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Inmediata	Alta	5 meses	S2-2025	95%
7	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	Inmediata	Alta	3 meses	S1-2022	65%
8	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Inmediata	Alta	6 meses	S1-2022	60%
9	PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.	Mediano plazo	Media	15 meses	S2-2023	40%
10	PCS-GI-17	Iniciativas para la simulación de ataques y pruebas de seguridad	Mediano plazo	Media	16 meses	S2-2024	30%
11	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.	Inmediata	Alta	5 meses	S2-2022	25%
12	PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético.	Inmediata	Media	10 meses	S1-2023	10%
13	PCS-GI-11	Iniciativas para la implementación de la gestión de la seguridad de los endpoint.	Mediano plazo	Baja	15 meses	S2-2024	5%
14	PCS-GI-12	Iniciativas para el fortalecimiento de la identidad y gestión de acceso.	Corto Plazo	Media	25 meses	S2-2024	5%
15	PCS-GI-13	Iniciativas para la gestión del acceso privilegiado en los sistemas de la CCSS	Mediano plazo	Media	16 meses	S1-2025	5%
16	PCS-GI-18	Iniciativas para la implementación de la gestión de la seguridad en la nube.	Mediano plazo	Baja	8 meses	S2-2024	2%
17	PCS-GI-06	Iniciativas para el desarrollo de una estrategia de respaldos institucional	Largo Plazo	Baja	8 meses	S2-2025	2%
18	PCS-GI-16	Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software.	Corto Plazo	Media	21 meses	S1-2023	0%
19	PCS-GI-19	Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.	Corto Plazo	Alta	6 meses	S1-2023	0%

20	PCS-GI-20	Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.	Corto Plazo	Alta	14 meses	S1-2024	0%
21	PCS-GI-14	Iniciativas para el establecimiento e implementación de las líneas base de seguridad.	Mediano plazo	Baja	9 meses	S1-2025	0%
22	PCS-GI-08	Iniciativas para la definición de una arquitectura de ciberseguridad que se alinee con los objetivos de la DTIC.	Largo Plazo	Baja	11 meses	S2-2025	0%
23	PCS-GI-22	Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC.	Mediano plazo	Baja	15 meses	S2-2025	0%

Fuente: Elaboración propia con información aportada en los oficios GG-DTIC-7306-2023, GG-DTIC-3964-2022 y documento PCS-ENT029

En el cuadro anterior se observa un total de 5 iniciativas cumplidas al 100% correspondientes a las iniciativas: 1, 4, 15, 21 y 23. De estas se identifica el cumplimiento de la iniciativa 21 *"Iniciativas para el aprovechamiento de los acuerdos nacionales e internacionales para potenciar el conocimiento y desarrollo de la ciberseguridad en la CCSS"* la cual tenía un plazo de cumplimiento al I semestre del 2025, con una prioridad definida baja, y una etapa de implementación del mediano plazo.

Respecto a lo anterior, en el oficio citado, para esta iniciativa se indicó lo siguiente:

> *"Se tiene como punto de contacto el MICITT, a través del CSIRT nacional, por medio del cual se aprovecha todos los acuerdos nacionales e internacionales.*
>
> *Producto de las gestiones realizadas por este ente rector, se ha implementado en infraestructura institucional, herramientas como Cisco Umbrella y microClaudia del CERST del Gobierno Español. Asimismo, se ha aprovechado procesos de capacitación ofrecidos a través de la Fundación Omar Dengo enfocados en ciberseguridad.*
>
> *Finalmente aprovechando los convenios internacionales del MICITT, se ha tenido apoyo de la Embajada del Gobierno de Estados Unidos, con asesorías brindadas por el Comando Sur".*

Si bien el Plan de Ciberseguridad establece en caso de que algún grupo de iniciativas se pueda ejecutar antes de lo indicado, debe ajustarse como parte del proceso de revisión de la hoja de ruta interpretándose como un beneficio para el desarrollo del plan de ciberseguridad, sin embargo, no se ha realizado el ajuste a la hoja de ruta por cuanto no se ha efectuado una revisión de ésta, fuera de la propuesta de reforzamiento del Plan.

Por otro lado, considerando el avance de ejecución de las iniciativas de acuerdo al tiempo estimado para su finalización, se identificó que 11 iniciativas se debieron de implementar del II semestre del 2021 al II semestre del 2023, de las cuales solo 4 (36%) registran un 100% de ejecución, determinándose además 2 iniciativas con 0% de avance (16 y 19) una con 10% (07) y otra con 25% (05) esta última debió estar finalizada para el II semestre del 2022, tal y como se observa:

Cuadro N° 3
Porcentaje de avance en la implementación de las iniciativas que integran la hoja de ruta del Plan de Ciberseguridad cuyo tiempo estimado de ejecución se estableció del 2021 al 2023
31 de octubre 2023

	Iniciativa	Descripción Iniciativa	Etapa implementación	Prioridad	Plazo estimado	T. Estimado	% Avance octubre 2023
1	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.	Inmediata	Alta	10 meses	S2-2021	100%
2	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Inmediata	Alta	6 meses	S1-2022	60%
3	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	Inmediata	Alta	3 meses	S1-2022	65%
4	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Inmediata	Alta	6 meses	S2-2022	100%
5	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.	Inmediata	Alta	5 meses	S2-2022	25%
6	PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético.	Inmediata	Media	10 meses	S1-2023	10%
7	PCS-GI-16	Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software.	Corto Plazo	Media	21 meses	S1-2023	0%
8	PCS-GI-19	Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.	Corto Plazo	Alta	6 meses	S1-2023	0%
9	PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral	Inmediata	Alta	15 meses	S1-2023	100%
10	PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.	Mediano plazo	Media	15 meses	S2-2023	40%
11	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Inmediata	Alta	38 meses	S2-2023	100%

Fuente: Elaboración propia con información aportada en los oficios GG-DTIC-7306-2023, GG-DTIC-3964-2022 y documento PCS-ENT029

Al analizar el avance por etapa de implementación se tiene que 9 de las 23 iniciativas se identificó con una etapa de implementación inmediata, de estas 4 registran un 100% de cumplimiento y hay dos iniciativas que registran un cumplimiento inferior al 50% como lo es la iniciativa 05 con un 25% de ejecución, y la iniciativa 7 con un 10% de ejecución, tal y como se observa en el siguiente cuadro:

Cuadro N° 4
Porcentaje de avance en la implementación de las iniciativas que integran la hoja de ruta del Plan de Ciberseguridad cuya etapa de implementación es inmediata
31 de octubre 2023

	Iniciativa	Descripción Iniciativa	Etapa implementación	Prioridad	Plazo estimado	T. Estimado	% Avance octubre 2023
1	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.	Inmediata	Alta	10 meses	S2-2021	100%
2	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Inmediata	Alta	6 meses	S1-2022	60%
3	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	Inmediata	Alta	3 meses	S1-2022	65%
4	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Inmediata	Alta	6 meses	S2-2022	100%
5	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.	Inmediata	Alta	5 meses	S2-2022	25%
6	PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético.	Inmediata	Media	10 meses	S1-2023	10%
7	PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral	Inmediata	Alta	15 meses	S1-2023	100%
8	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Inmediata	Alta	38 meses	S2-2023	100%
9	PCS-GI-10	Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Inmediata	Alta	5 meses	S2-2025	95%

Fuente: Elaboración propia con información aportada en los oficios GG-DTIC-7306-2023, GG-DTIC-3964-2022 y documento PCS-ENT029

Asimismo, al analizar las iniciativas por prioridad se tiene que 10 de las 23, registran una prioridad alta, de las cuales 4 presentan 100% de ejecución, registrándose 2 iniciativas con 0% de avance (19 y 20), y la iniciativa 5 con el 25% como se observa:

Cuadro N° 5
Porcentaje de avance en la implementación de las iniciativas que integran la hoja de ruta del Plan de Ciberseguridad cuya prioridad es alta
31 de octubre 2023

	Iniciativa	Descripción Iniciativa	Etapa implementación	Prioridad	Plazo estimado	T. Estimado	% Avance octubre 2023
1	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.	Inmediata	Alta	10 meses	S2-2021	100%
2	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Inmediata	Alta	6 meses	S1-2022	60%
3	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	Inmediata	Alta	3 meses	S1-2022	65%
4	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Inmediata	Alta	6 meses	S2-2022	100%

5	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.	Inmediata	Alta	5 meses	S2-2022	25%
8	PCS-GI-19	Iniciativas para la implementación de la gestión de la seguridad con los proveedores de servicios.	Corto Plazo	Alta	6 meses	S1-2023	0%
9	PCS-GI-23	Iniciativas para el fortalecimiento de la seguridad perimetral	Inmediata	Alta	15 meses	S1-2023	100%
11	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Inmediata	Alta	38 meses	S2-2023	100%
12	PCS-GI-20	Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.	Corto Plazo	Alta	14 meses	S1-2024	0%
22	PCS-GI-10	Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Inmediata	Alta	5 meses	S2-2025	95%

Fuente: Elaboración propia con información aportada en los oficios GG-DTIC-7306-2023, GG-DTIC-3964-2022 y documento PCS-ENT029

AVANCE DE LAS 10 INICIATIVAS PRIORITARIAS

El Proyecto de Ciberseguridad estableció para su fase 6, la definición de 10 iniciativas prioritarias, las cuales debían realizarse de primeras de acuerdo con su criticidad y riesgo. Al respecto, se identificó que actualmente de estas, únicamente 2 registran un 100% de ejecución, asimismo se presentan iniciativas como la 05 que debía estar lista en el II semestre del 2022 y presenta un 25% de ejecución, y la iniciativa 07 que se tenía el plazo al I semestre de 2023 y registra un 10% tal como se observa:

Cuadro N° 6
Porcentaje de avance en la implementación de las 10 iniciativas prioritarias del Plan de Ciberseguridad
31 de octubre 2023

	Iniciativa	Descripción Iniciativa	Etapa implementación	Prioridad	Plazo estimado	T. Estimado	% Avance octubre 2023
1	PCS-GI-02	Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	Inmediata	Alta	6 meses	S1-2022	60%
2	PCS-GI-01	Iniciativas para la formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	Inmediata	Alta	6 meses	S2-2022	100%
3	PCS-GI-07	Iniciativas para la implementación de la gestión del riesgo cibernético.	Inmediata	Media	10 meses	S1-2023	10%
4	PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.	Mediano plazo	Media	15 meses	S2-2023	40%
5	PCS-GI-11	Iniciativas para la implementación de la gestión de la seguridad de los endpoint.	Mediano plazo	Baja	15 meses	S2-2024	5%
6	PCS-GI-15	Iniciativas para el desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	Inmediata	Alta	38 meses	S2-2023	100%
7	PCS-GI-10	Iniciativas para implementar el Plan de Concientización en Ciberseguridad.	Inmediata	Alta	5 meses	S2-2025	95%
8	PCS-GI-09	Iniciativas para la implementación de la gestión de vulnerabilidades y parches.	Mediano plazo	Media	15 meses	S2-2023	40%
9	PCS-GI-17	Iniciativas para la simulación de ataques y pruebas de seguridad	Mediano plazo	Media	16 meses	S2-2024	30%

10	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.	Inmediata	Alta	5 meses	S2-2022	25%

Fuente: Elaboración propia con información aportada en los oficios GG-DTIC-7306-2023, GG-DTIC-3964-2022 y documento PCS-ENT029

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en el punto "VI. Calidad de los Procesos Tecnológicos" indican:

> *"La institución debe implementar prácticas que permitan controlar los procesos organizacionales, posibilitando la mejora continua de productos y servicios, buscando asegurar la satisfacción de las necesidades institucionales, manteniendo estándares de documentación de los lineamientos requeridos, esquemas para la medición del desempeño y control sobre la vigencia de las prácticas aplicables a los procesos.*
>
> *Igualmente, debe generar servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo de los procesos que habilitan la gestión de las tecnologías de información".*

Asimismo, en la descripción del Perfil del Proceso, la misma norma indica:

> *"**PERFIL DEL PROCESO***
>
> *Para asegurar que se realiza una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, debe asegurarse que cumpla con el siguiente perfil:*
>
> *(…)*
> *2. La propiedad del proceso debe estar claramente establecida, sobre el diseño, interacción con otros procesos**, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora**.*
>
> *3. **Debe estar claramente establecida la secuencia de actividades de forma lógica, consecuente, flexible, y escalable de forma tal que produzca los resultados esperados**, considerando el manejo de excepciones y emergencias. (…)*
>
> *6. **Deben contar con indicadores de desempeño, de tal forma que permitan identificar el nivel de logro de las metas**. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique". (la negrita no es del original)*

Las Normas de Control Interno para el Sector Público, en el punto 4.5 "Garantía de eficiencia y eficacia de las operaciones establecen:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. 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"*

Asimismo, en el punto 4.5.2 Gestión de Proyectos se indica:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.

Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:

(…)

c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.
d. El establecimiento de un sistema de información confiable, oportuno, relevante y competente para dar seguimiento al proyecto.
e. La evaluación posterior, para analizar la efectividad del proyecto y retroalimentar esfuerzos futuros"

El Máster Danilo Hernández Monge, subdirector a.i. de la DTIC, el 8 de noviembre de 2022 mediante oficio GG-DTIC-6407-2022, remitido a la Auditoría Interna, respecto a las limitantes en la implementación del Plan de Ciberseguridad indicó:

"a) La capacidad institucional para llevar adelante la ejecución del plan de ciberseguridad, iniciando con la limitada capacidad de recurso humano, no solo en la Subárea de Seguridad en TI, sino también, en el resto de las áreas de la DTIC, teniendo en consideración que llevar adelante iniciativas del plan, requiere la participación de funcionarios de otras instancias de la Dirección, las cuales, tienen la misma problemática de capacidad instalada, que impiden tener la participación e involucramiento requerido según las necesidades de desarrollo de cada iniciativa. Sobre este particular, cabe señalar que actualmente la subárea de seguridad cuenta con 4 recursos, siendo uno de ellos la Ing. Vanessa Carvajal Carmona como jefatura de la subárea. Las cargas de trabajo que estos recursos atienden, hacen que su esfuerzo no pueda ser a tiempo completo, más aún, muchas veces sus aportes a la atención del plan, se realiza como recargo a las tareas de la operativa diaria que deben atender, aspecto que ha impactado en la ejecución eficiente y eficaz, tanto de las funciones diarias sustantivas como de las encomendadas dentro de las iniciativas del plan, lo anterior sin considerar los problemas asociados a la salud de los funcionarios como estrés, cansancio, desmotivación, síndrome burnout, entre otros (…)".

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informáticas, al respecto señalaron:

"El Ing. Daniel Berrocal hace una introducción señalando los factores de éxito, que en lo personal considera que han afectado el desarrollo del Plan de Ciberseguridad, primero se tuvo un ciberataque el año anterior, eso hizo que la mayor parte de los recursos de la DTIC, basaran su trabajo operativo en el levantamiento de los servicios, cuando se logró levantar los servicios no se terminó el problema, ya que surgieron una serie de recomendaciones de mejores prácticas, no solo de seguridad, si no de Redes, Sistemas de Información, y todos en general, por ahí se empieza a perder el esfuerzo sobre el programa de Ciberseguridad y entran a regir otros temas prioritarios como el levantamiento de los servicios, aplicar mejoras en servicios, infraestructura y demás.

Se ha tenido la problemática de la rotación de Sub-Gerentes, comenzando por la suspensión que le hicieron a Don Robert Picado, posteriormente estuvo Roberto Blanco, luego Doña Idannia Mata que se pensionó, luego siguió Don Eithel, pero este fue nombrado como Gerente de Logística, y ahora la tiene como recargo Danilo Hernández. Se debe considerar, además, que el principal patrocinador de este plan es el Consejo Tecnológico, y este también ha sufrido cambios ante la rotación de los gerentes, ya que desde que se inició este tema, el único que se ha mantenido es Don Jaime Barrantes, gerente de Pensiones, de ahí en adelante todos los gerentes han variado.

Ustedes tienen conocimiento un cronograma donde vienen cada una de las iniciativas, si uno analiza a grandes rasgos ese cronograma es lo que deberíamos estar cumpliendo, sin embargo, debajo de ese cronograma está el Consejo Tecnológico donde se llevó una solicitud de recurso humano para poder llevar el Cronograma adelante, donde se informó la necesidad de 12 recursos, de estos 12 recursos que se han solicitado, no se ha recibido apoyo de ni recurso humano para poder avanzar y desarrollar cada una de estas iniciativas. Si dentro de un año ustedes me consultan por el avance de cada una de ellas, mi respuesta va a ser la misma, ya que nosotros tenemos 7 personas en la Subárea de Seguridad, pero el trabajo operativo del día a día es prioritario ya que se debe mantener operativo los servicios, mitigar los diferentes riesgos, monitorear todo lo que se necesita mediante el contrato del SOC por ejemplo, esto no quiere decir que el Plan de Ciberseguridad no tenga importancia, tiene mucha importancia y es necesario realizarlo, sin embargo no podemos descuidar todo el trabajo operativo, por lo que hasta que no se dote de ese recurso humano, el otro año probablemente yo les estaría diciendo lo mismo".

La situación descrita, respecto a los porcentajes de avance en la implementación de las iniciativas de la hoja de ruta, compromete la efectividad y el alcance del Plan de Ciberseguridad e indica una posible desviación temporal de la ejecución de este, poniendo en riesgo la Ciberseguridad y Seguridad de la Información de la Institución, al presentarse la posibilidad de disminuir la protección frente a posibles amenazas. La falta de adherencia a los plazos establecidos refleja la necesidad de revisar y reestructurar la gestión del proyecto, para garantizar una implementación más eficiente y oportuna, asegurando así la protección adecuada de los activos digitales y la información sensible que se administra en la CCSS.

4. CONTROLES EN LA GESTIÓN DEL PLAN DE CIBERSEGURIDAD

Se identificaron oportunidades de mejora en los controles implementados por parte de la Administración Activa en torno a la gestión de la ejecución del Plan de Ciberseguridad y su hoja de ruta. Lo anterior de acuerdo a los siguientes aspectos:

2.1 REFERENTE A LOS INFORMES PERIÓDICOS SOBRE EL AVANCE EN LA IMPLEMENTACIÓN DE LAS INICIATIVAS DE LA HOJA DE RUTA

Se identificó la existencia de informes de avance en la implementación de la hoja de ruta y sus 23 iniciativas, no obstante, estos no presentan un análisis de las métricas definidas en el Plan de Ciberseguridad que midan el desempeño y que permitan dar el adecuado seguimiento a dicho plan, aunado a una revisión anual de estas métricas ya definidas.

Lo anterior considerando que el documento PCS-ENT-029 "Plan de Ciberseguridad para la Caja Costarricense de Seguro Social (CCSS) en el punto 7.4 Etapa 4 Métricas indica:

"En esta sección se proponen las métricas de desempeño que permitirán hacer seguimiento al plan de ciberseguridad de la CCSS, comparándolo contra el estado deseado definido y, además, darán visibilidad a la DTIC acerca de la efectividad de las funciones de ciberseguridad establecidas y la habilidad de lograr los objetivos.

Es importante mencionar que estas métricas deberán revisarse anualmente para asegurar que aportan la información relevante y requerida para el plan de ciberseguridad. A su vez, es importante asegurar

que las funciones continúan siendo relevantes para los objetivos de ciberseguridad, para lo cual se debe revisar anualmente la matriz de trazabilidad de funciones y objetivos de ciberseguridad indicados en el punto 7.2.2.1 del presente documento, para asegurar que las métricas plasmadas son convenientes para el plan de ciberseguridad. Por otra parte, dentro de los ajustes anuales se pueden agregar métricas, aumentar las frecuencias de medición a medida que se aumentan los niveles de madurez y valorar si es posible lograr automatización. En la Tabla 19 se presentan las métricas para el plan de ciberseguridad.

Función	Métrica
Gestión de riesgos de ciberseguridad	Porcentaje de riesgos de ciberseguridad que superan el nivel de riesgo aceptable, que han sido mitigados en los últimos 6 meses
Inteligencia de amenazas	Porcentaje de amenazas analizadas semestralmente
Gobierno de ciberseguridad	Porcentaje de lineamientos de ciberseguridad, directrices, estándares y procedimientos revisados en los últimos 12 meses
Gestión de programa de ciberseguridad	Porcentaje de avance real vrs planificado del programa de ciberseguridad
Seguimiento de auditorías de ciberseguridad y regulaciones	Porcentaje de acciones correctivas implementadas en los últimos 12 meses
Gestión de riesgos de terceros	Porcentaje de contratos de terceros que posean las cláusulas de ciberseguridad
Análisis y monitoreo de tendencias y del entorno	Cantidad de tendencias de ciberseguridad analizadas trimestralmente
Capacitación y concientización en Ciberseguridad	Porcentaje de usuarios que completaron la capacitación y concientización sobre ciberseguridad en los últimos 6 meses. Porcentaje de usuarios que identificaron un ataque en las pruebas de ingeniería social.
Administración de herramientas de ciberseguridad	Porcentaje de activos críticos que deben ser protegidos por una herramienta de ciberseguridad versus los activos críticos que son administrados por ciberseguridad
Administración de la identidad y el acceso	Porcentaje de cuentas inactivadas oportunamente
Seguridad de datos (Respaldos, borrado seguro, redes)	Porcentaje de pruebas de restauración realizadas satisfactoriamente.
	Porcentaje de computadoras portátiles / activos de información sensibles cifrados
Arquitectura de Ciberseguridad	Porcentaje de soluciones de ciberseguridad que cumplen con la arquitectura tecnológica de seguridad diseñada
Gestión de vulnerabilidades y parches	Variación del número de vulnerabilidades detectadas en los re escaneos Porcentaje de parches implementados satisfactoriamente
Pruebas de penetración	Cantidad de pruebas de penetración realizadas trimestralmente
Desarrollo seguro	Cantidad de pruebas de seguridad del código fuente realizados anualmente
Gestión y monitoreo de eventos	Porcentaje de activos monitoreados
Detección / Prevención de intrusos	Cantidad de veces que atacantes intentaron obtener acceso no autorizado
Respuesta y seguimiento de incidentes de ciberseguridad	Porcentaje de incidentes de ciberseguridad mitigados satisfactoriamente
Recuperación ante desastres de ciberseguridad	Porcentajes de planes de recuperación ante desastres de ciberseguridad probados durante los últimos 12 meses
Seguridad en la nube	Porcentaje de cumplimiento de los proveedores de la nube

Tabla 19: Métricas del plan de ciberseguridad

"

2.2 INCONSISTENCIAS EN LOS PORCENTAJES EN EL AVANCE DE LAS INICIATIVAS REPORTADOS POR LA DTIC

Producto del informe bimensual solicitado por el Máster Robert Picado, Sub-Gerente de la DTIC, la subárea de Seguridad Informática mediante oficio GA-DTIC-3443-2022, efectuó el "Análisis de iniciativas del Plan Ciberseguridad" donde presentaron el avance de cada una de las 23 iniciativas, por lo que esta Auditoría realizó un comparativo con los informes efectuados anteriormente a saber:

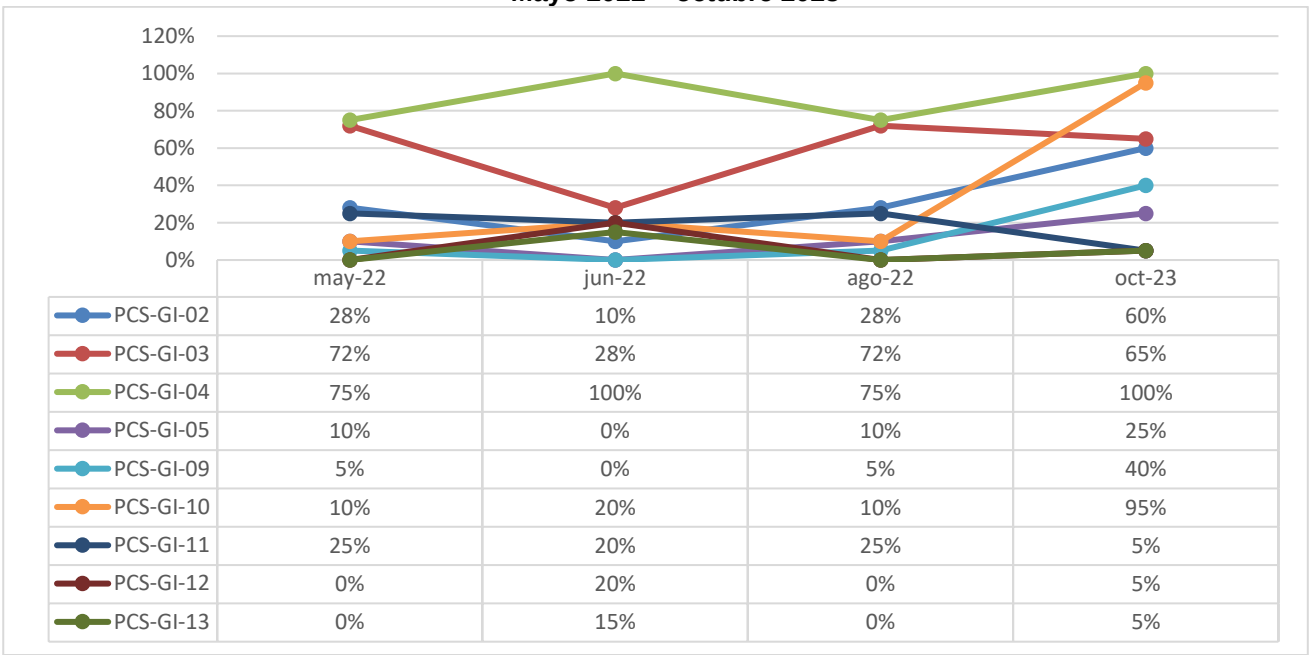
- Oficio GG-DTIC-2376-2022 del 6 de mayo de 2022 "Informe de Seguimiento "Implementación Plan de Ciberseguridad a abril 2022", suscrito por Máster Mayra Ulate Rodríguez, jefe del área de Calidad y Seguridad Informática y Máster Danilo Hernández Monge, subdirector a.i. de la DTIC.

- Oficio GG-DTIC-2892-2022 del 9 de junio de 2022 "Sobre, lo solicitud de Iniciativas Contratación 2019LA-000001-1150 "Plan de Ciberseguridad", suscrito por Máster Mayra Ulate Rodríguez, jefe del área de Calidad y Seguridad Informática.

- Oficio GG-DTIC-3964-2022 del 18 de agosto de 2022 "Atención oficio GG-DTIC-3375-2022 referido al AD-ATIC-046-2022", suscrito por Máster Vanessa Carvajal Carmona, jefe de la subárea de Seguridad Informática y Máster Danilo Hernández Monge, subdirector a.i. de la DTIC.

Al respecto se identificaron inconsistencias en los porcentajes reportados por el área de Seguridad y Calidad en torno al avance de las 23 iniciativas, lo anterior por cuanto en 9 de ellas se presentan disminución de estos en comparación con los periodos anteriores, según el siguiente detalle:

Gráfico N° 6
Iniciativas con disminución en los porcentajes de avances en relación con informes anteriores
Plan de Ciberseguridad y su Hoja de Ruta
Mayo 2022 – octubre 2023



	may-22	jun-22	ago-22	oct-23
PCS-GI-02	28%	10%	28%	60%
PCS-GI-03	72%	28%	72%	65%
PCS-GI-04	75%	100%	75%	100%
PCS-GI-05	10%	0%	10%	25%
PCS-GI-09	5%	0%	5%	40%
PCS-GI-10	10%	20%	10%	95%
PCS-GI-11	25%	20%	25%	5%
PCS-GI-12	0%	20%	0%	5%
PCS-GI-13	0%	15%	0%	5%

Fuente: elaboración propia

Como se observa, iniciativas como la 03 pasa de avances de 72% a 28% luego a 72% nuevamente para reportar un 65% actualmente, de igual forma la iniciativa 11 que pasó de 25% a 20% y luego a 25% nuevamente para reportar un 5% actualmente.

2.3 RESPECTO A LA DEFINICIÓN DE ROLES Y RESPONSABILIDADES PARA LA IMPLEMENTACIÓN DE LAS 23 INICIATIVAS DEL PLAN DE CIBERSEGURIDAD

Se identificó que mediante oficio GG-DTIC-5735-2021 del 28 de setiembre de 2021, el Máster Roberto Blanco Topping, Sub-Gerente a.i. de la Dirección de Tecnologías de Información y Comunicaciones en ese momento, conformó el equipo de trabajo para la implementación de las 23 iniciativas del Plan de Ciberseguridad, dicho equipo de trabajo quedó conformado en ese momento por el Máster Christian Chacón Rodríguez, Subdirector de la Dirección de Tecnologías de Información y Comunicaciones, la Máster Mayra Ulate Rodríguez, jefe del área de Seguridad y Calidad Informática, la Licda. Vanessa Carvajal Carmona, jefe a.i. de la Subárea de Seguridad en Tecnologías de Información y la Máster Ericka Sánchez Solís funcionaria de la Subárea de Seguridad en Tecnologías de Información, sin embargo no se definieron las responsabilidades de cada uno de los integrantes del equipo asignado para la implementación de las iniciativas.

Asimismo, en la propuesta del Plan de Fortalecimiento del Proyecto de Ciberseguridad, si bien se definieron nuevas iniciativas, en dicho documento tampoco se establecieron los roles y responsabilidades de las personas encargadas de implementarlas.

El documento PCS-ENT-029 “Plan de Ciberseguridad” en el apartado recomendaciones señala:

"Con base en los resultados del diseño del plan de ciberseguridad, se presentan recomendaciones generales que podrían ayudar a la implementación de los proyectos en la Caja Costarricense de Seguro Social. (…)

.

• Considerar la creación de un equipo responsable de la administración de los grupos de iniciativas o proyectos del programa de Plan del Ciberseguridad de la CCSS. Se recomienda definir los roles y responsabilidades que tendrá cada uno de los funcionarios para la implementación, desarrollo y mantenimiento del Programa de Ciberseguridad de la CCSS.

• Establecer un taller de revisión anual de la hoja de ruta, con el objetivo de analizar si las iniciativas siguen siendo convenientes para la Institución y ajustar su prioridad"

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en el punto "IX. Gestión de Proyectos que Implementan Recursos Tecnológicos" detallan:

"La institución debe gestionar los proyectos que permitan habilitar sus iniciativas para el logro de los objetivos estratégicos, satisfaciendo los requerimientos y en cumplimiento con términos de calidad, tiempo, presupuesto y uso óptimo de los recursos, de acuerdo con las buenas prácticas y estándares preestablecidos".

Asimismo, en la descripción del Perfil del Proceso, la misma norma indica:

"PERFIL DEL PROCESO

Para asegurar que se realiza una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, debe asegurarse que cumpla con el siguiente perfil:

(…)

*2. La propiedad del proceso debe estar claramente establecida, sobre el diseño, interacción con otros procesos**, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora**. (…)*

*6. **Deben contar con indicadores de desempeño, de tal forma que permitan identificar el nivel de logro de las metas**. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique". (la negrita no es del original)*

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informáticas, señalaron:

"(…) sobre este tema existe una deuda, porque realmente se tenía que dar un control de avance, sin embargo como parte del análisis para hacer la gestión de métricas, resultó este oficio 3443, sin embargo se está en ese proceso de retomar la parametrización de actividades para llegar y definir esto, Don Daniel ya tomó parte en el asunto, yo el pasado 29 de agosto mandé un oficio a los sub alternos, delegando responsabilidades entre estos temas, establecer el control de avance, y se estableció plazo al próximo 29 de setiembre para la presentación de este tema en concreto.

Hay tareas que como tal y como se recibió el mismo proyecto, no existe una parametrización correcta, donde por ejemplo para la iniciativa 23 que habla de seguridad perimetral, aunque estamos llevando un proceso de implementación de esta tecnología que ya está en fase 2, no hay una parametrización correcta para indicar cuando porcentaje de avance se tiene, realmente sobre este tema se está generando este informe con actualización de métricas como tal (…)".

La Ing. Vanessa Carvajal Carmona, jefe de la subárea de Seguridad Informática en su momento indicó a esta Auditoría:

> *"No se definieron roles ni actividades, se nos conformó en ese equipo, que en lo personal considero debió ser todo el personal de la subárea, pero no se definió un rol para cada uno, solo en otros oficios aparte de este, donde se definen como líder de proyecto a Mayra y a mí como encargada general del contrato"*

Asimismo, la Ing. Ericka Sánchez Solís, funcionaria de la Subárea de Seguridad en Tecnologías de Información, indicó:

> *"Dentro de mi designación como parte del equipo de implementación de las 23 iniciativas del Plan de Ciberseguridad, de acuerdo con el oficio GG-DTIC-5735-2021, con fecha 28 de setiembre 2021, no se me definió ningún tipo de rol o responsabilidad sobre las acciones a llevar a cabo como parte de dicha comisión (…).*
>
> *El trabajo realizado por mi persona en la implementación de las 23 iniciativas del Plan de Ciber-seguridad ha estado relacionado directamente con las funciones y responsabilidades que me han sido solicitadas como funcionaria de la Subárea de Seguridad en Tecnologías de Información (SSTI), a cargo de la Licda. Vanessa Carvajal Carmona, Encargada General de este contrato".*

Las situaciones descritas se presentan – entre otras causas – ante el faltante de recurso humano que debe estar a cargo de la ejecución de las iniciativas de la hoja de ruta, que permita mantener un adecuado control y seguimiento mediante la implementación de las métricas definidas, así como de la necesidad de tener un mejor registro del avance de las iniciativas que garantice que la información aportada en los informes sea la real, aunado a lo anterior los cambios presentados por los funcionarios que integran el equipo de trabajo conformado para la implementación de las iniciativas han impactado en el adecuado seguimiento de la hoja de ruta.

La ausencia de mediciones que evalúen el desempeño mediante las métricas definidas y correctas dificulta la capacidad de entender el progreso real y la eficacia de las acciones implementadas, impidiendo identificar áreas de mejora, ajustar estrategias oportunas y eficientemente, así como tomar decisiones informadas. Asimismo, la carencia de definición de responsabilidades para el equipo encargado de ejecutar estas actividades aumenta el riesgo de que las tareas se realicen de manera desorganizada o incluso se omitan por completo.

Estas omisiones no solo comprometen la capacidad de la Institución para adaptarse a cambios en las amenazas cibernéticas, sino que también limita la posibilidad de garantizar una protección óptima de los activos digitales y la información sensible de la CCSS, al no ejecutarse el Plan de Ciberseguridad con los controles adecuados para lograr los objetivos propuestos.

5. RESPECTO AL PLAN DE CIBERSEGURIDAD REFORZADO

Se evidenció que el "Plan de Fortalecimiento Proyecto de Ciberseguridad" no se ha aprobado formalmente por parte del Consejo Tecnológico, aunado a que no se identificó el cumplimiento de las etapas definidas en la normativa institucional para el aval por parte de ese Órgano Colegiado, de tal forma que se garantice que la Institución dispone de los recursos para llevar a cabo la materialización del Plan reforzado y las iniciativas establecidas.

Al respecto, el Plan de Fortalecimiento del Proyecto de Ciberseguridad 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, donde indicaron que la documentación base para definir el Plan reforzado consideraba:

- Plan de Ciberseguridad PSC-ENT-029 (23 iniciativas que se vienen desarrollando desde la aprobación del Plan en diciembre de 2020).
- Oportunidades de mejora identificadas en la Evaluación de Riesgos, Infraestructuras Críticas (ICC),

realizado por la Organización de Estados Americanos (OEA) y el MICITT.
- 115 recomendaciones planteadas por los distintos servicios de consultorías con lo que actualmente cuenta la DTIC (Deloitte, Microsoft, GBM) y el apoyo brindado por el MICITT, bajo convenios con otras instituciones.
- Informes y recomendaciones brindadas por la Auditoría Interna sobre temas de Ciberseguridad.

Seguidamente, se expuso las recomendaciones para el reforzamiento del Plan de Ciberseguridad, en el cual se considera la ejecución de acciones en torno a 28 iniciativas correspondientes a temas de Ciberseguridad y 6 de Seguridad de la Información, para un total de 34 iniciativas.

Los acuerdos tomados por el Consejo Tecnológico en dicha sesión fueron:

1 Que la DTIC coordine con las instancias correspondientes los procesos de inducción virtual a través del CENDEISSS para personal de primero ingreso a la CCSS, sobre temas de ciberseguridad.

2 A cada Gerencia se le solicita hacer análisis para asignar personal informático a la labor de ciberseguridad conducida desde DTIC.

3 Presentar un cronograma de recursos y presupuesto requerido como parte del plan de fortalecimiento en Ciberseguridad.

Como se observa, en los acuerdos tomados por dicho Órgano Colegiado, no se otorga una aprobación formal del Plan reforzado, esto toma relevancia por cuanto las nuevas iniciativas presentan componentes tecnológicos, por lo que debe considerarse efectuar las gestiones acordes a lo establecido en el Modelo de Toma de Decisiones de tal forma que se garantice la disponibilidad de recursos para su ejecución. En razón de lo anterior, las nuevas iniciativas no se identifican en los informes de avance efectuados por la Subárea de Seguridad Informática.

La Directriz para la Gobernanza de TIC en su punto 8.5 indica:

> *"La definición del valor y beneficios de los proyectos e inversiones en TIC se llevará a cabo desde su planteamiento inicial, por medio de caso de negocio, siendo estos considerados como elementos clave para el análisis, priorización y aprobación por parte del Consejo Tecnológico.*
>
> *El valor y beneficios de cada inversión en TIC se definirán de forma clara y concreta, utilizando elementos cuantificables que faciliten el monitoreo y verificación de la generación de valor y el logro de los beneficios, tanto durante la ejecución de la inversión como posterior a su conclusión.*
>
> *(…) A través del proceso institucional de Banco de Iniciativas y Portafolio Institucional de Proyectos (específicamente en lo que se refiere a proyectos con componente TIC) se establecen los procedimientos para realizar la aprobación de los proyectos con componente TIC, cuya evaluación debe tomar en consideración el valor y beneficios asociados con una iniciativa, a efectos de determinar la conveniencia de su desarrollo."*

Asimismo, en el punto 8.6 de la misma directriz se establece:

> *"Toda iniciativa e inversión en TIC debe contar con datos que soporten la necesidad, justificando su desarrollo en términos de la utilidad de la solución/ servicio TIC y de la rentabilidad de su adquisición y/o uso.*
>
> *El análisis de la factibilidad de los requerimientos de soluciones tecnológicas es una responsabilidad conjunta entre la DTIC y las áreas usuarias; donde a estas últimas compete justificar la necesidad de contar con la funcionalidad y el análisis operativo, mientras que la DTIC se enfoca en la factibilidad*

técnica de implementar, soportar y mantener las soluciones. El análisis de factibilidad financiero deberá ser desarrollado en conjunto por la unidad solicitante y el Equipo Multidisciplinario de Transformación en TIC, tomando en consideración las disposiciones que a nivel de la Gerencia Financiera sean establecidas para tal efecto.

Es responsabilidad de la DTIC la administración consolidada de todos los requerimientos de tecnologías de la información y comunicaciones de la CCSS tanto a nivel estratégico como operativo, apoyado en un procedimiento y herramientas estándar para el análisis y aprobación de requerimientos de tecnologías de la información comunicaciones".

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado I. Gobernanza, señala:

"La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales".

Esta auditoría mediante oficio AI-2115-2023 del 23 de octubre de 2023, le consultó al Máster Robert Picado Mora, Sub-Gerente de la DTIC, informar si el "Plan de Fortalecimiento del Proyecto de Ciberseguridad" fue formalmente aprobado por el Consejo Tecnológico, y de no ser así, en que etapa se encuentra para su aprobación, recibiéndose respuesta mediante oficio GG-DTIC-7462-2023 del 7 de noviembre de 2023, suscrito por el Máster Daniel Berrocal Zúñiga, jefe a.i. del área de Seguridad y Calidad Informática, indicando:

"Es por lo anterior que se procede a atender los puntos indicados en mencionado oficio:

Punto No. 1 Informar si el "Plan de Fortalecimiento del Proyecto de Ciberseguridad" fue formalmente aprobado por el Consejo Tecnológico, y de no ser así, en que etapa se encuentra para su aprobación.

Respuesta

Se adjunta la Minuta 002-2023 de fecha 23 de enero de 2023, es importante indicar que no se cuenta con la firma de todos los asistentes debido a que por los cambios en las gerencias no se ha logrado conseguir el total de firmas".

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informáticas, señalaron:

"En cuanto a esa minuta de esa sesión del Consejo Tecnológico, no nos la han trasladado, incluso hemos estado detrás de esa minuta desde hace meses y lo que se nos indica es que han tenido problemas con la firma, por lo que no tenemos conocimiento de los acuerdos tomados. Desde que hemos ocupado los actuales puestos, no hemos recibido información de dichos acuerdos, sin embargo, se va a validar si previamente se solicitó algo, y si los compañeros que estuvieron antes lo remitieron".

El 20 de febrero de 2023 mediante oficio GG-DTIC-0932-2023, los ingenieros Ericka Sánchez Solís, jefe a.i. de la Subárea de Seguridad Informática, Luis Diego Peña Ledezma, jefe subárea Administración de Proyectos, Adriana Moreira Madrigal, analista de la Subárea de Administración de Proyectos, Esteban Zamora Chaves,

asistente de despacho, y Danilo Hernández Monge, subdirector a.i. todos de la Dirección de Tecnologías de Información y Comunicaciones, le informaron al Máster Eithel Corea Baltodano, Sub Gerente de la DTIC, sobre aspectos comentados en la sesión del Consejo Tecnológico en el que se presentó el Plan Fortalecido de Ciberseguridad, indicando:

> *"Cada una de las iniciativas que lo componen, será abordada de acuerdo con la hoja de ruta establecida, del año 2022 al 2026, para lo cual es indispensable contar con los recursos humanos que permitan, no solo la ejecución de las iniciativas del periodo, sino lograr los análisis y estudios correspondientes para los subsecuentes periodos a atender.*
>
> *(…)*
>
> *Al respecto, es importante destacar, que cada una de estas iniciativas deben ser desarrolladas a partir de la fecha de inicio prevista según la priorización detallada en el documento remitido a la gerencia el pasado 18 de noviembre, y el tiempo que cada una de estas implica, depende de los estudios y análisis que deben ser desarrollados para las mismas, especialmente las que se integran a partir del ciberataque en el programa fortalecido, dado que estas aún no han sido desarrolladas por la escasez del recurso humano disponible para la ejecución de las iniciativas y sus análisis.*
>
> *Esto quiere decir, que la planificación de la DTIC contempla el inicio de las iniciativas en el periodo definido, no obstante, su tiempo de ejecución variara dependiendo de la complejidad de esta y de los recursos asignados para su ejecución (recursos humanos, financieros, tecnológicos, etc.)."*

La situación descrita en torno a la aprobación oficial del reforzamiento del Plan de Ciberseguridad afecta la formalización y ejecución de estrategias críticas de ciberseguridad identificadas producto del hackeo perpetrado durante el 2022, dejando a la Institución expuesta a riesgos potenciales. Además, la omisión de las etapas definidas en la normativa institucional referente a los proyectos con componentes TIC propuestos, afecta la capacidad de evaluar la viabilidad y el impacto de estos, lo que podría llevar a una asignación inadecuada de recursos y a la implementación de soluciones subóptimas.

6. RESPECTO AL RECURSO HUMANO REQUERIDO PARA LA IMPLEMENTACIÓN DEL PLAN DE CIBERSEGURIDAD

Se determinó que la DTIC ha identificado como limitante para el cumplimiento efectivo en la implementación de las iniciativas de la hoja de ruta del Plan de Ciberseguridad, el faltante de recurso humano, por lo que en el Plan Reforzado de Ciberseguridad se propuso la conformación del equipo de Ciberseguridad de la red integrada de servicios TIC, no obstante, el mismo no se ha materializado.

El Plan de Fortalecimiento del Proyecto de Ciberseguridad, en el punto 10.4 "Necesidad de recursos" indica:

> *"A raíz de llevar a cabo el análisis y la agrupación de las iniciativas, se contabilizaron en total 35 iniciativas o grupos documentados, los cuales al implementarse permitirán que las brechas entre el estado actual y el estado objetivo deseado puedan subsanarse y fomentar una robusta gestión de la ciberseguridad en la Caja Costarricense de Seguro Social.*

El impacto de no realizar estas iniciativas genera que la CCSS no tenga los insumos necesarios para el desarrollo e implementación del programa de ciberseguridad, el cual se deriva del Plan de Ciberseguridad del proyecto denominado "Servicios Profesionales para desarrollar un Plan de Ciberseguridad para la CCSS, Licitación Abreviada 2019LA-000001-1150", por lo tanto, gran parte de las iniciativas que se desean llevar a cabo para alcanzar el estado objetivo de madurez no podrán implementarse dejando a la CCSS sin avances para robustecer la gestión de la ciberseguridad en la institución y por ende, a los activos tecnológicos expuestos a las constantes amenazas que emergen día a día.

A continuación, se detallan un conjunto de elementos que forman parte los insumos requeridos para lograr las metas propuestas en cada una de las iniciativas, las cuales, sin el apoyo de estas, no será posible el cumplimiento de los objetivos. (Ver Anexo 2)

Dicho Plan fue presentado al Consejo Tecnológico el 23 de enero de 2023 por parte del Ing. Danilo Hernández Monge, subdirector de la DTIC, y la Ing. Ericka Sánchez Solís, analista en sistemas de la DTIC, en el cual como acuerdo tercero tomado por el Consejo Tecnológico se indicó:

"3. Presentar un cronograma de recursos y presupuesto requerido como parte del plan de fortalecimiento en Ciberseguridad".

Al respecto, esta auditoría mediante oficio AI-2115-2023 del 23 de octubre de 2023, le consultó al Máster Robert Picado Mora, Sub-Gerente de la DTIC, informar el estado de dicho cronograma de recursos y presupuesto, recibiéndose respuesta mediante oficio GG-DTIC-7462-2023 del 7 de noviembre de 2023, suscrito por el Máster Daniel Berrocal Zúñiga, jefe a.i. del área de Seguridad y Calidad Informática, indicando:

"Se adjunta oficio GG-DTIC-0932-2023 de fecha 20 de febrero de 2023, en el cual se presenta la aplicación sobre aspectos comentados en la sesión del Consejo Tecnológico en el que se presentó el Plan de Fortalecimiento del Programa de Ciberseguridad, entre ellos:
I. Sobre la gestión del plan de Ciberseguridad fortalecido bajo la figura de Programa.
II. Sobre las capacidades de Recurso Humano con perfil informático a nivel institucional".

Al revisar el oficio en mención, en el punto "II. Sobre las capacidades de Recurso Humano con perfil informático a nivel institucional" se indica:

"(…)

Este equipo ha sido diseñado como un grupo de trabajo conformado por 12 RRHH, adicionales al rol de la coordinación del equipo que estaría a cargo de la jefatura de la Subárea de Seguridad Informática de la DTIC, 2 de la DTIC y 10 procedentes de otras unidades. Así entonces se propone la conformación del equipo bajo la siguiente consideración:

• 2 funcionarios representantes de la Subárea de Seguridad Informática adicionales a la jefatura de dicha subárea que tendrá a cargo la coordinación del equipo de trabajo. Como se comentó esto implica la asignación del 100% de la capacidad actual con que cuenta dicha subárea.
• 4 miembros representantes de CGIs de Gerencia Médica
• 2 miembros representantes de CGIs de Gerencia Financiera
• 4 miembros, 1 representante de cada CGI gerencial de Pensiones, Logística, Infraestructura y Administrativa.
Estos recursos, deben estar asignado 100% a las funciones requeridas para atender las necesidades del Programa en lo que a las iniciativas de ciberseguridad se refiere. Estos 10 recursos corresponden a tan solo el 3% de la totalidad de profesionales informáticos distribuidos fuera de la DTIC.

Esta propuesta, se fundamenta en considerar las capacidades de recurso humano con perfil informático con que cuentan las distintas Gerencias y que, para los efectos, se puede visualizar en el siguiente gráfico que muestra la cantidad de funcionarios y el porcentaje referido a la totalidad de la capacidad institucional.

(…)

Para mayor ampliación cabe señalar que desde la perspectiva del perfil de las plazas, considerando dos grupos, técnicos y profesionales, teniendo referido que el recurso requerido para la conformación del equipo de ciberseguridad de la red integrada de servicios TIC debe contar con perfil profesional, tal como se indicó anteriormente, aun cuando no sea experto en temas de ciberseguridad, se muestra el siguiente cuadro:

Tabla N°1
Plazas con perfil informático a nivel institucional
A setiembre 2022

Perfil De Plazas	Gerencia Medica	Gerencia Administrativa	Gerencia Logística	Gerencia Pensiones	Gerencia Financiera	Gerencia General	Git	Total General
TÉCNICO (NO PROFESIONAL)	184	6	18	11	30	9	1	259
PROFESIONAL	203	6	6	14	46	8	14	297

Fuente: GG-DAGP-1736-2022, noviembre 2022.

De la tabla anterior, se desprende que existe un total de 297 plazas con perfil profesional, correspondientes a Analistas de Sistemas 2,3,4 y puestos de Jefaturas, en diversas gerencias, de las cuales el 68% correspondiente a 203 plazas profesionales se encuentran adscritas a la Gerencia Médica, mientras que el 32% restante se ubican en las restantes gerencias. El detalle se presenta a continuación:

Tabla N°2
Plazas con Perfil Profesional fuera de la DTIC
A setiembre 2022

Puesto	Gerencia Logística	Gerencia Médica	Gerencia Pensiones	Gerencia Infraestructura	Gerencia General	Gerencia Financiera	Gerencia Administrativa	Total general
Analista en Sistemas 2 en TIC	1	54	2	2		2	2	63
Analista en Sistemas 3 en TIC		13	1			1		15
Analista en Sistemas 4 en TIC	5	99	11	10	8	43	3	179
Jefe Centro de Gestión informática Gerencial							1	1
Jefe Centro de Gestión TIC 1		21						21
Jefe Centro de Gestión TIC 2		15						15
Jefe en TIC 1				1				1
Jefe en TIC 2		1		1				2
Total general	**6**	**203**	**14**	**14**	**8**	**46**	**6**	**297**

Fuente: GG-DAGP-1736-2022, noviembre 2022.

(…)Así mismo, cabe informar que, como parte de los esfuerzos de capacitación en diferentes temas relacionados con las TICs, que se han gestionado en coordinación con los Centros de Gestión Informática, se han desarrollado tres actividades de capacitación en temas ciberseguridad, para un total de 97 participaciones, los cuales se detallan en el siguiente cuadro:

Tema	Gerencia Administrativa	Gerencia Financiera	Gerencia General	Gerencia Infraestructura y Tecnologías	Gerencia Logística	Gerencia Médica	Gerencia Pensiones	Junta Directiva	Total, general
Fundamentos de Ciberseguridad CSX	3	14	2	2		21	2	1	45
ISO 27001 Y 270002 Seguridad Informática	4	4	4	1	1	5	2	1	22
Marco de Ciberseguridad NIST	2	2	2	2		19	1	2	30
Total	9	20	8	5	1	45	5	4	97

En consideración de esta distribución de perfiles informáticos fuera de la DTIC, se presenta la propuesta de conformación del equipo de ciberseguridad de la red integrada de servicios TIC, lo anterior considerando que la Institución dispone de recursos capacitados cuyas funciones pueden ser redistribuidas entre los restantes recursos de cada gerencia para fortalecer las funciones de ciberseguridad, aspecto que adquirió mayor relevancia a raíz del ciberataque por el impacto que generó en la prestación de servicios"

No obstante, a lo anterior, no se evidenció avance en la conformación del equipo de trabajo propuesto, y tampoco el cumplimiento del acuerdo tercero de la sesión del Consejo Tecnológico, en razón de que el Plan Reforzado de Ciberseguridad no ha sido aprobado, y que la minuta de la sesión del Consejo Tecnológico donde se presentó este Plan ante el faltante de firmas de algunos integrantes no ha tomado firmeza los acuerdos contenidos en ella.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, en el apartado "VII Recursos Humanos" señalan:

"La institución debe disponer de un proceso formal que le permita gestionar los recursos humanos de acuerdo con las necesidades institucionales, en apego a directrices y regulaciones según aplique. Las prácticas deben apoyar el reclutamiento, selección, contratación, inducción y capacitación continua según lo requerido".

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002, en el apartado 8.10 establece:

"La Agenda Digital Institucional constituye el portafolio integral e institucional de proyectos e inversiones con componente TIC, esto permite una adecuada coordinación de los recursos requeridos para su desarrollo, al tiempo que aporta visibilidad de los esfuerzos que la CCSS está realizando en transformación y operación de servicios TIC. Por lo anterior, se asignarán recursos para su desarrollo únicamente a aquellos proyectos que hayan sido valorados y aprobados conforme a las disposiciones y procedimientos establecidos en la presente directriz y en los procesos Banco de Iniciativas y Portafolio de Proyectos TIC (específicamente en lo que se refiere a proyectos con componente TIC)."

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informáticas, al respecto señalaron:

"En cuanto a esa minuta de esa sesión del Consejo Tecnológico, no nos la han trasladado, incluso hemos estado detrás de esa minuta desde hace meses y lo que se nos indica es que han tenido problemas con la firma, por lo que no tenemos conocimiento de los acuerdos tomados. Desde que hemos ocupado los actuales puestos, no hemos recibido información de dichos acuerdos, sin embargo, se va a validar si previamente se solicitó algo, y si los compañeros que estuvieron antes lo remitieron.

¿Qué ha cambiado cuando se solicitaron los recursos al día de hoy?, básicamente se dio un recurso el 26 de julio, sin embargo este recurso no es para este tema del Plan de Ciberseguridad, sino que es para apoyar en la parte operativa, principalmente para la atención de todo lo relacionado con la mesa de servicios, pero el recursos humano para apoyar el Plan de Ciberseguridad, la respuesta no se ha materializado, aunque nos han dicho en una ocasión que nos iban a apoyar con algunos recursos en TIC de la Gerencia Médica, no se ha materializado, ahora en las últimas dos semanas Don Juan Ignacio nos solicitó que realizáramos un inventario del recurso humano con perfil TIC a nivel central y nivel Institucional para que apoye la operativa, pero ese es una trabajo que apenas estamos desarrollando y al final no puedo dar seguridad de que se llegue a materializar, podría ser que en el corto o mediano plazo se den cambios en las direcciones, gerencias o en esta área y eso quede en el olvido, por lo que no se ha brindado el apoyo con recurso humano para el desarrollo del programa de Ciberseguridad".

El faltante de recurso humano para implementar las iniciativas del Plan de Ciberseguridad compromete la ejecución eficaz de este, limitando la capacidad de la Institución para desarrollar y mantener medidas efectivas de protección aumentando así la vulnerabilidad frente a amenazas cibernéticas, lo que podría materializar nuevos ataques como el presentado en mayo de 2022.

7. SOBRE LA NORMATIVA EN MATERIA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

Se evidenció que la normativa vigente en materia de Ciberseguridad y Seguridad de la Información no se ha actualizado, presentándose incluso Políticas y Normas que datan del 2007 y 2008, pese a la existencia de una iniciativa en la hoja de ruta del Plan de Ciberseguridad que busca su actualización y subsanar brechas existentes.

Al respecto, la Administración Activa mantiene vigentes las siguientes normas:

- Políticas Institucionales de Seguridad Informática TIC-Seguridad-001, octubre 2007. Avalado por el Comité Gerencial de Tecnologías de Información de la CCSS, en sesión Nº23 celebrada el 30 del mes de octubre del año 2007.
- Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002, abril 2008.
- Normas Institucionales en Tecnologías de Información y Comunicaciones, abril 2012.

En cuanto a la hoja de Ruta del Plan de Ciberseguridad, la iniciativa PCS-GI-02 *"Iniciativas para el desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes"*, tiene como objetivo estandarizar y actualizar la normativa y los lineamientos con el Plan de Ciberseguridad y desarrollar la faltante para la gestión de la ciberseguridad en la institución, formalizando los canales de comunicación de dichos lineamientos para que los funcionarios se mantengan informados de cambios que se realicen sobre estos, no obstante y a pesar de que esta iniciativa tenía un tiempo estimado de ejecución al I semestre del 2022, actualmente registra un 60% de avance.

Aunado a lo anterior, la hoja de ruta también define la iniciativa PCS-GI-20 *"Iniciativas para la implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas"* que tiene como objetivo implementar los controles de ciberseguridad aplicables a la CCSS con base en el marco de referencia de NIST y cumplir con los requisitos legales y regulatorios en materia de ciberseguridad en la Institución y si bien esta tiene un plazo estimado de cumplimiento al I semestre del 2024, actualmente registra un avance del 0%.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, en el apartado *"Perfil del proceso"* detallan:

> *5. Debe disponer de lineamientos y planes debidamente formalizados, revisados, actualizados, aprobados, almacenados, comunicados, publicados y utilizados en forma consecuente, que establezcan las directrices y acciones requeridas. Los lineamientos deben estar accesibles y asegurar el claro entendimiento por parte de los responsables de su aplicación, así como de las partes interesadas. Los lineamientos se constituyen por:*
>
> *(…)*
> *● Políticas y directrices que brinden la información necesaria en el más amplio nivel de detalle sobre las normas y mecanismos que se deben cumplir*
> *● Normas que definan los propósitos generales dentro de un marco o política regulatoria, indicando lo que debe hacerse para su cumplimiento de acuerdo con el entorno de gestión y alcances establecidos por la organización.*
> *● Procedimientos, para tareas específicas de tipo operativo-administrativo, indicando el cómo se lleva a cabo una actividad o un proceso describiendo con alto grado de detalle el modo de realizar las actividades principales y la parametrización de los componentes e integrantes del proceso que describen.*
> *(…)*

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. (…)"*

En oficio GA-DTIC-3443-2022 del 2 de junio 2023, el Lic. Erick Vindas Umaña, jefe a.i. de la Subárea de Seguridad de Tecnologías de Información informa al Ing. Daniel Berrocal Zúñiga, jefe a.i. Área Seguridad y Calidad Informática, el alcance de las iniciativas relacionadas, detallando lo siguiente:

> ***"No. Iniciativa 2: Alinear la normativa y lineamientos que actualmente posee la CCSS al Plan de Ciberseguridad, a las sanas prácticas que imperen en la industria y al marco de referencia NIST.***
>
> *Actividad 1: Alinear la normativa y lineamientos que actualmente posee la CCSS al Plan de Ciberseguridad, a las sanas prácticas que imperen en la industria y al marco de referencia NIST.*
>
> *Actividad 2: Identificar y desarrollar los lineamientos requeridos para abordar brechas identificadas con la normativa existente.*
>
> - *Actividades pendientes u observaciones: Las propuestas de la Política e Instructivos se encuentran pendientes de revisión por el Despacho de la DTIC."*
>
> *Actividad 3: Formalizar y aprobar los lineamientos por parte de la DTIC.*
>
> - *Actividades pendientes u observaciones: Las propuestas de la Política e Instructivos se encuentran pendientes de revisión por el Despacho de la DTIC.*
>
> *Actividad 4: Incluir la nueva normativa en el esquema documental de Gobernanza y Gestión de las TIC.*
>
> - *Actividades pendientes u observaciones: Depende avance de Gobernanza*
>
> *Actividad 5: Implementar una herramienta o mecanismo que permita llevar el control de revisiones y modificaciones a los lineamientos.*
>
> - *Actividades pendientes u observaciones: Preguntar a Luis Diego Camacho si el posee una herramienta para revisión y modificación de normativa Tener pendiente quien va a asumir la operativa.*
>
> *Actividad 6: Formalizar los canales de comunicación interna para mantener al personal informado sobre los lineamientos que disponga la CCSS en materia de seguridad informática.*
>
> *Actividad 7: Actualizar en los distintos sistemas según lo solicitado en la nueva normativa y otros controles que se basan en los lineamientos actuales, para que se mantengan en concordancia, por ejemplo, revisar que los requerimientos de contraseñas que solicita el AD concuerde con los lineamientos de contraseñas seguras.*
>
> - *Actividades pendientes u observaciones: Documento línea base de Vanessa indica: Pendiente hacer un documento para llevar el control*

Actividad 8: Establecer un mecanismo periódico para la verificación de la aplicación de la normativa en los distintos sistemas de información institucionales.

- *Actividades pendientes u observaciones: Tener pendiente quien va a asumir la operativa, Documento línea base de Vanessa indica: Pendiente hacer un documento para llevar el control.*

No. Iniciativa 20. Alinear la normativa y lineamientos que actualmente posee la CCSS al Plan de Ciberseguridad, a las sanas prácticas que imperen en la industria y al marco de referencia NIST.

Actividad 1: Definir el catálogo de servicio, protocolos de atención y el acuerdo de nivel de servicio para los servicios de ciberseguridad que se incluyan en la mesa de servicio, considerando usuarios finales y centros de gestión informática, imperen en la industria y al marco de referencia NIST.

Actividad 2: Realizar la petición al área encargada de administrar la mesa de servicio para adicionar los servicios de ciberseguridad en la herramienta.

Actividad 3: Comunicar a los involucrados los servicios de ciberseguridad que serán provistos a través de la herramienta de la mesa de servicios.

Actividad 4: Revisión Anual de los Protocolos de atención y Acuerdos de Servicios

- *Actividades pendientes u observaciones: Documento línea base de Vanessa indica: Primer Revisión se hizo en octubre- noviembre 2021".*

El 26 de octubre de 2022, se efectúa entrevista a la Licda. Vanessa Carvajal Carmona, en ese momento jefe de la Subárea de Seguridad en Tecnologías de Información de la Direccion de Tecnologías de Información y Comunicaciones (DTIC) con el propósito de recabar información y aclarar aspectos relacionados con el avance en la implementación del Plan de Ciberseguridad, en la cual comenta los siguientes aspectos:

- *(…) La otra es la renovación de la normativa y política de seguridad, que están desactualizadas ya que estas son del 2008, en esto tuvimos dos temas, se comenzó con la documentación nueva con un formato, luego la dirección de planificación cambió el formato, ya no se llamaba lineamiento y pasaron a ser instructivos, esa política la estuvimos coordinando con la dirección de Planificación y eso llevó bastantes meses, para poder avanzar con los demás iniciativas se tenía que tener bien definida esta política, incluso esta todavía no está lista, lo mandaron a la Dirección y la devolvieron para nuevamente socializarla y revisarla, con bases a los eventos que se han presentado.*

La situación descrita en torno a la desactualización de la normativa expone a la Institución a riesgos de seguridad, dado que las regulaciones obsoletas podrían no abordar adecuadamente las nuevas y emergentes amenazas cibernéticas. La demora en la actualización de estas normativas resalta la necesidad de agilizar este proceso para fortalecer las defensas de ciberseguridad y garantizar el cumplimiento de estándares actualizados que protejan de manera efectiva los datos y sistemas de la CCSS.

8. RESPECTO A LA COORDINACIÓN CON EL ÁREA DE INGENIERÍA EN SISTEMAS EN MATERIA DE CIBERSEGURIDAD

Se determinaron aspectos de mejora en torno a la coordinación del área de Seguridad y Calidad con el área de Ingeniería en Sistemas, lo anterior debido a que esta última identificó la necesidad de iniciar un proceso de contratación relacionado con software seguro, donde el objetivo principal es la incorporación de prácticas de desarrollo seguro en la fábrica de software y en los equipos de desarrollo, no obstante, el Plan de Ciberseguridad tiene en ejecución la iniciativa PCS-GI-16 denominada "*Iniciativas para la integración de la ciberseguridad a la metodología de desarrollo de software"* en la cual se define como objetivo, adoptar una cultura DevSecOps en la CCSS que permita combinar buenas prácticas en el desarrollo de software con herramientas y metodologías ágiles que integren la ciberseguridad en cada etapa del desarrollo y que esto formalice una cultura de seguridad por diseño.

Dicha iniciativa se le asignó una prioridad media, y una etapa de implementación a corto plazo, con un tiempo estimado de ejecución al I semestre de 2023, no obstante, actualmente registra un avance del 0%.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, en el apartado "XI Seguridad y Ciberseguridad" señalan:

> *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.*

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. (…)"*

El Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad en TIC, mediante oficio GG-DTIC-7306-2023 presentaron el avance de las iniciativas del Plan Táctico de Ciberseguridad, al respecto para la iniciativa 16 señalaron:

> *"Si bien la iniciativa tenía una proyección de inicio para el 2022 según cronograma del Plan de Ciberseguridad, aspectos como el ciberataque sufrido, los traslados de la DTIC a diferentes gerencias, atención de prioridades de negocio, escaso recurso humano, han generado atrasos en el inicio del desarrollo de actividades.*
>
> *Se estará realizando un reajuste en el cronograma y al mismo tiempo se estará coordinando con el Área Ingeniería de Sistemas para el desarrollo de esta iniciativa.*

El Ing. Sergio Paz Morales, jefe a.i. del área de Ingeniería en Sistemas en ese momento, en entrevista efectuada el 21 de setiembre de 2023, indicó:

> *"En lo que respecta a la iniciativa incorporada en el plan de ciberseguridad, actualmente estamos proponiendo una contratación que tiene como objetivo abordar la temática de software seguro y así estar preparados en el ámbito de ciberseguridad. Esto como producto de hace algunos meses atrás donde nos reunimos con la SSTI y al exponernos cuál era la iniciativa más bien nos generó una preocupación ya que la asesoría que ellos pretendían contratar venía a decirnos o asesorarnos sobre qué era lo que nos hacía falta, pero ya nosotros teníamos ese conocimiento, lo que ocupamos es más bien poner en marcha la solución.*
>
> *De momento, esto implica que quizás no sea necesario invertir tiempo en el desarrollo de la Iniciativa 16 del Plan de Ciberseguridad por parte del equipo de la SSTI. Nuestra propuesta abarca un alcance más amplio e incluye asesoría y acompañamiento. El objetivo principal de esta iniciativa es la incorporación de prácticas de desarrollo seguro en la fábrica de software y en los equipos de desarrollo. Inicialmente, consideramos incluirla como parte de una adquisición en el ámbito de Control de Calidad (QA), pero identificamos un riesgo considerable de que la compra no se completara a tiempo.*

Por lo tanto, al final decidimos formular una adquisición por separado. Esta elección también nos proporciona la ventaja de tener criterios de evaluación contrastados, incluso en caso de que otro proveedor, diferente al actual proveedor de QA, se involucre en el proceso".

La falta de coordinación entre áreas que gestionan componentes tecnológicos impide la integración de prácticas de seguridad desde la etapa inicial del desarrollo de software en este caso, lo que aumenta significativamente el riesgo de vulnerabilidades y debilidades en los programas diseñados. La ausencia de una alineación adecuada entre áreas de la DTIC compromete la capacidad de la Institución para producir y mantener tecnología robusta y protegida, dejándola expuesta a potenciales brechas de seguridad y amenazas informáticas.

9. GESTIÓN Y TRATAMIENTO DE RIESGOS

Se determinó que en el Plan de Ciberseguridad se realizó la identificación de riesgos en torno al proyecto y a la Ciberseguridad Institucional, asimismo en el último informe trimestral presentado el 31 de octubre de 2023 sobre el estado de las 23 iniciativas de la hoja de ruta, no obstante, se evidenciaron oportunidades de mejora en el tratamiento de estos en torno a la medición, evaluación, control y seguimiento.

Al respecto, el 31 de octubre de 2023 mediante oficio GG-DTIC-7306-2023, los Ingenieros Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad y Erick Vindas Umaña, jefe de subárea presentaron al Máster Robert Picado Mora, Sub-Gerente de la DTIC el informe trimestral del estado actual de las 23 iniciativas del Plan Táctico de Ciberseguridad para la Caja Costarricense de Seguro Social, en el cual se evidenciaron riesgos de alto y medio impacto que se mantienen actualmente, entre los cuales se citan:

- No se están respetando los prerrequisitos incluidos en las fichas técnicas elaboradas por la empresa PwC que se encuentran contenidas en documento PCS-ENT-029 "Plan de Ciber seguridad" así como el orden cronológico/lógico en la ejecución de las iniciativas.

- El Plan Táctico de Ciberseguridad tiene como pilar el Sistema Gestor de Seguridad de la Información, el cual corresponde a una de las iniciativas a desarrollar en el Programa de Gobernanza de las TIC y Seguridad de la Información, esto es un riesgo en la consecución del Plan de Cibertic, así como el desarrollo de servicios y soluciones desarticuladas a nivel institucional.

- No se dispone del Modelo de Gobernanza de la Ciberseguridad aprobado, el cual es requerido para que el proyecto brinde continuidad, seguimiento y evolución, así como la correspondiente alineación en caso de presentarse desvíos respecto a los objetivos planteados inicialmente, si bien existe una vinculación indirecta a nivel de general de dicho Programa con el Plan Táctico de Ciberseguridad, podría no respetarse dicha dependencia durante el desarrollo de las actividades.

- Las políticas de seguridad deben ser dictadas por el negocio y es lo que permitirá a la DTIC el alineamiento estratégico, sin embargo, estas tienen alta dependencia de la iniciativa de seguridad de la información institucional y a pesar de haberse actualizado, siguen sin aprobación.

- Falta de asignación y formalización de roles y responsabilidades asociados a las funciones, dominios y capacidades de ciberseguridad y el no contar con recursos expertos y capacitados en todos los dominios de ciberseguridad, lo cual es clave para poder habilitar las capacidades requeridas.

- No contar con un esquema de clasificación de la información a nivel institucional, el cual dicte las pautas requeridas en cuanto a confidencialidad, integridad y disponibilidad de la información, lo cual es clave para poder establecer y diseñar los controles de ciberseguridad requeridos, de acuerdo con el nivel de criticidad que posea el activo de información.

- Diez iniciativas incluyen dentro de sus proyectos la adquisición de herramientas o soluciones tecnológicas, por ende, se debe analizar y decidir que unidades lideraran los posibles procesos de contratación, contemplando aspectos de disponibilidad de recurso humano, conocimiento técnico sobre la herramienta que se pretende adquirir en el proceso licitatorio, inversión o presupuesto a asignar, unidad encargada o responsable de la gestión de la herramienta en el ámbito operativo.

Las Normas Técnicas de Control y Gestión de las TI, emitidas por el MICITT señalan en el apartado IV. Gestión de riesgos tecnológicos, refieren:

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

Las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgo Institucional (SEVRI), establecen

> *"4.4 "Evaluación de riesgos": "Los riesgos analizados deberán ser priorizados de acuerdo con criterios institucionales dentro de los cuales se deberán considerar, al menos los siguientes:*
>
> *a) el nivel de riesgo,*
> *b) grado en que la institución puede afectar los factores de riesgo;*
> *c) la importancia de la política, proyecto, función o actividad afectado; y*
> *d) la eficacia y eficiencia de las medidas para la administración de riesgo existentes.*
>
> *4.5 Administración de riesgos: A partir de la priorización de riesgos establecida, se debe evaluar y seleccionar la o las medidas para la administración de cada riesgo, de acuerdo con criterios institucionales que deberán contener al menos los siguientes:*
>
> *a) la relación costo-beneficio de llevar a cabo cada opción;*
> *b) la capacidad e idoneidad de los entes participantes internos y externos a la institución en cada opción;*
> *c) el cumplimiento del interés público y el resguardo de la hacienda pública; y*
> *d) la viabilidad jurídica, técnica y operacional de las opciones".*

Al respecto 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(...)"*

Así mismo, esta Ley en su artículo 14, referente a la Valoración del Riesgo, establece:

> *"En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes: a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos. b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos. c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable. d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar"*

El 2 de junio de 2023, mediante oficio GA-DTIC-3443-2022 el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad en TIC, le remitió al Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática, el resultado del análisis de actividades pendientes por desarrollar vinculadas con las iniciativas del Plan Táctico de Ciberseguridad para la Caja Costarricense de Seguro Social, en el cual indicó:

> *"(…) dada la importancia que tienen actualmente los temas de Ciberseguridad a nivel global y en la Institución, es menester de esta Subárea comunicar diversos aspectos detectados durante el presente análisis, los cuales podrían impactar tanto la ejecución de las iniciativas plasmadas en el documento del Plan de Ciberseguridad, como la continuidad las actividades a desarrollar a nivel operativo en las diversas unidades de la Dirección de Tecnologías de Información y Comunicaciones (DTIC). El detalle se muestra a continuación: "* (ver Anexo 3)

Asimismo, en dicho oficio en el apartado "Riesgos y/o limitantes generales identificados", indicó que, en el documento del Plan de Ciberseguridad, la empresa PwC determinó diversos riesgos que podrían afectar la ejecución del Proyecto y limitar a la Institución en torno al alcance de un modelo de ciberseguridad deseado, además que en el análisis efectuado de las 23 iniciativas se determinaron riesgos adicionales que podrían incidir en el éxito de su ejecución y desarrollo.

Al respecto, esta Auditoría mediante entrevista consultó al Ing. Daniel Berrocal Zúñiga, jefe del área de Seguridad y Calidad Informática y el Ing. Erick Vindas Umaña jefe de la subárea de Seguridad informática, si se dio respuesta al oficio GA-DTIC-3443-2022 respecto a los riesgos identificados, señalando:

> *"Se escaló a Danilo Hernández como subdirector y Sub-Gerente a cargo y se tiene programado la sesión de trabajo el 14 de setiembre de 2023".*

Debilidades en la gestión de riesgos, podrían generar la materialización de eventos que impactan tanto la ejecución de las iniciativas plasmadas en el documento del Plan de Ciberseguridad, como la continuidad las actividades a desarrollar a nivel operativo, si bien se han identificado los posibles riesgos, la ausencia de un tratamiento o gestión efectiva de los mismos deja a la Institución vulnerable ante potenciales amenazas, lo que podría llevar a una subestimación, dejando a la CCSS expuesta a incidentes de seguridad cibernética.

CONCLUSIONES

La Ciberseguridad y la Seguridad de la Información son aspectos fundamentales para garantizar la adecuada gobernanza y gestión de una organización moderna, su importancia radica en garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas críticos.

En un entorno digital altamente interconectado como el actual, la presencia de amenazas cibernéticas es latente y en constante evolución, por lo que un Plan de Ciberseguridad correctamente gestionado no solo es esencial para salvaguardar la información sensible y los activos digitales de la Institución, sino que también garantiza la continuidad operativa y la confianza de los usuarios de los servicios que presta la CCSS.

Así mismo, dicho plan se convierte en la base sobre la cual se construyen todas las estrategias de defensa digital, estableciendo no solo directrices y procedimientos para detectar, prevenir y responder a posibles amenazas cibernéticas, sino que también asegura la alineación de los objetivos de seguridad con las metas generales de la Institución.

Por lo anterior es que resulta de importancia particular y estratégica que el actual Plan de Ciberseguridad que se encuentra implementando la CCSS, se lleve a cabo utilizando una metodología estructurada para la gestión de proyectos donde se controle procesos de alcance, tiempo y costo y con el seguimiento adecuado, que evite comprometer la eficiencia y eficacia de la protección de los activos y datos institucionales, por lo que también se deben de utilizar los mecanismos de control en torno a los proyectos con componentes tecnológicos que tiene definido la Institución como lo es el AGEDI de tal forma que se lleve un mejor control en el avance de la implementación de dicho Plan.

Si bien la DTIC ha hecho el esfuerzo por robustecer el Plan de Ciberseguridad actual producto del ataque cibernético sufrido el 31 de mayo de 2022, es importante que el mismo cumpla con las etapas definidas institucionalmente y su aprobación se realice por parte del Consejo Tecnológico sustentado en decisiones técnicas que garanticen la adecuada implementación y gestión de este.

Un aspecto crítico que está afectando la correcta gestión del Plan de Ciberseguridad, es la carencia de recurso humanos especializado y la falta de equipos dedicados a la implementación de las iniciativas definidas, lo que ha impedido el cumplimiento eficaz de las tareas y ha generado retrasos en la ejecución del plan de seguridad, lo anterior pese a que se acordó en sesión de Consejo Tecnológico efectuar un cronograma de recursos y presupuesto requerido, tarea que a la fecha tampoco se ha llevado a cabo.

Asimismo, la deficiencia en la actualización de normativas y la falta de coordinación entre distintas áreas, como la de ingeniería de sistemas y la de seguridad informática podría generar brechas en la implementación de iniciativas de ciberseguridad. La desconexión entre estas áreas clave ha debilitado la integración de prácticas de seguridad desde etapas tempranas de desarrollo, exponiendo a la organización a posibles vulnerabilidades en el software y sistemas.

Finalmente, la inadecuada gestión de riesgos en torno a la Ciberseguridad y Seguridad de la Información podría tener un impacto importante en la operativa Institucional. A pesar de identificar los posibles riesgos, la falta de un debido tratamiento de riesgos con un enfoque estructurado para su medición, evaluación, control y seguimiento podría dejar a la Institución vulnerable a amenazas cibernéticas potenciales, subestimando el impacto y la gestión de dichos riesgos.

RECOMENDACIONES

AL MÁSTER ROBERT PICADO MORA, SUBGERENTE DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O QUIEN EN SU LUGAR OCUPE EL CARGO

1. Efectuar la revisión del “Plan de Fortalecimiento de Ciberseguridad” propuesto el 23 de enero del 2023 ante el Consejo Tecnológico, considerando que el mismo no ha sido aprobado por dicho Órgano Colegiado para que se analice el replanteamiento de este, valorando entre otros aspectos que esa administración activa considere, los siguientes puntos:

    - Gestionar el Plan de Ciberseguridad y su hoja de ruta con una perspectiva de proyectos, analizando de manera detallada cada una de las iniciativas para determinar su alcance y factibilidad de implementación.
    - Se analice las iniciativas que deben estar incluidas en el AGEDI y se realice los procesos correspondientes definidos institucionalmente para que sean incorporadas en esta herramienta de control de proyectos
    - Mejorar los controles de la gestión del Plan de Ciberseguridad robusteciendo los informes periódicos de avance de las iniciativas, implementando las métricas adecuadas para la correcta medición de desempeño, y la definición de roles y responsabilidades en la ejecución de las iniciativas establecidas.

- Considerar la priorización de las iniciativas que debieron estar completadas al II semestre del 2023, entre ellas las relacionadas con la actualización de la normativa en materia de Ciberseguridad y Seguridad de la Información.
- Analizar las necesidades de otras áreas en torno a la Ciberseguridad de sus procesos sustantivos, para que se realicen las coordinaciones respectivas y la actualización de las iniciativas según corresponda
- Verificar la gestión y tratamiento de riesgos en torno a la Ciberseguridad de la CCSS

El replanteamiento del "Plan de Fortalecimiento de Ciberseguridad" que resulte debe ser presentado al Consejo Tecnológico para el trámite correspondiente de acuerdo a lo establecido en la normativa vigente.

Todo lo anterior de acuerdo a lo evidenciado en los hallazgos del 1 al 9 del presente estudio.

Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **4 meses**, a partir de la recepción del presente informe, la documentación que respalde la revisión del Plan de Fortalecimiento de Ciberseguridad donde se haya incluido los puntos anteriormente mencionados.

2. Llevar a cabo el cumplimiento de los acuerdos efectuados por el Consejo Tecnológico de la sesión del 23 de enero del 2023 referente a la presentación del cronograma de recursos y presupuesto requerido como parte del plan de fortalecimiento en Ciberseguridad, de tal forma que se valore las opciones de disponibilidad de recursos para la implementación de las iniciativas de la hoja de ruta del Plan de Ciberseguridad, el mismo debe ser enviado a la Gerencia General para su revisión, análisis y aprobación, lo anterior en concordancia a lo evidenciado en el **hallazgo 6** del presente estudio.

   Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **4 meses**, a partir de la recepción del presente informe, la documentación que respalde el cumplimiento de dichos acuerdos y la elaboración del cronograma de recursos y presupuesto.

En relación con las recomendaciones expuestas en el presente informe, en el plazo de 10 días hábiles[1] se deberá remitir a esta auditoría el "cronograma de acciones[2]" con las actividades o tareas, encargados designados y tiempo de ejecución previstos en función del plazo total acordado para el cumplimiento de cada una. Asimismo, se deberá informar periódicamente sobre los avances del cronograma y aportar las evidencias respectivas, a fin de que se pueda verificar el cumplimiento oportuno.

Se recuerda que, **si por motivos debidamente justificados**, durante la ejecución del cronograma la administración requiere ampliar el plazo de alguna recomendación, el jerarca o titular subordinado responsable de su cumplimiento, deberá solicitar formalmente la respectiva prórroga, **en tiempo y forma**, conforme lo establecido en el artículo 93 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, aportando además, el cronograma actualizado, conforme con el nuevo plazo que se esté solicitando y las actividades que presenten el respectivo retraso justificado.

El formato estandarizado del "Cronograma de acciones para el cumplimiento de recomendaciones" puede ser descargado del SIGA desde la ventana de inicio, en siguiente ícono  . Se solicita que; en el plazo señalado se remita el oficio de respuesta al informe, incluyendo como adjunto el "Cronograma de acciones para el cumplimiento de recomendaciones" adecuadamente completado, a través del SIGA, en el módulo de "Oficios" apartado "Respuesta informe", vinculándolo al número de informe (indicar # de informe). De esta misma forma, se remitirá posteriormente, la evidencia que constate los avances.

[1] Plazo máximo establecido en la Ley General de Control Interno (Art. 17 inciso d / Art. 36 inciso a), para iniciar la implantación de las recomendaciones de los informes de auditoría.
[2] Art. 68 del Reglamento de Organización y Funcionamiento de la Auditoría Interna.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 62 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 27 de noviembre de 2023 por medio de la Plataforma Microsoft Teams; de acuerdo con la convocatoria realizada por la Auditoría Interna, mediante oficio AI-2366-2023 del 27 de noviembre de 2023, estando presentes el Máster Robert Picado Mora, Sub Gerente de la Dirección de Tecnologías de Información y Comunicaciones, Máster Manuel Montillano Vivas, asesor de la Gerencia General, el Ing. Daniel Berrocal Zúñiga, jefe a.i. del área de Seguridad y Calidad y el Ing. Erick Vindas Umaña, jefe a.i. de la sub área de Seguridad Informática, Licda. Criselda M. Sánchez Rojas y Lic. Julián Gerardo Chaves Chaves, funcionarios del despacho de la DTIC.

En relación con los hallazgos presentados se emitieron los siguientes comentarios:

El Máster Robert Picado indica que, si la evaluación se hizo sobre las 23 iniciativas y no sobre las 34 del plan reforzado, porque el plan reforzado no ha sido aprobado, consulta si el plan original fue aprobado en su momento por algún foro, al respecto el Ing. Leonardo Díaz señala el Plan de Ciberseguridad forma parte de los entregables del proyecto de Gobernanza que fue aprobado en Junta Directiva y visto en Consejo Tecnológico.

El Ing. Daniel Berrocal respecto al hallazgo 6 hace referencia a que la minuta si se presentó pero que técnicamente lo que falta es la firma de la minuta por parte del Consejo Tecnológico, debido a que la fecha en que se presentó este plan reforzado, se realizó una serie de movimientos de Gerentes, donde dejaron minutas sin firmar.

El Máster Robert Picado indica que él vio las iniciativas, pero que incluso le dijo a Daniel Berrocal que esto hay que volver a presentarlo en el Consejo Tecnológico y no por un tema de forma si no por un tema de fondo, por lo que se le solicitó hacer una depuración de las iniciativas, hacer un consolidado con otras unidades, porque por ejemplo, todo el tema que ha venido trabajando Soporte Técnico, cuando la Caja tomó la decisión de tomar el tema de parcheo, esto forma parte de las iniciativas también, y había un tema de MicroClaudia, por lo que se ha venido realizando algunas depuraciones, por lo anterior es de la idea de que hay que presentarlo nuevamente.

El Ing. Daniel Berrocal, indica que inclusive parte de lo comentado por Don Robert, la gráfica que se mostró respecto a las inconsistencias en el reporte de las iniciativas, al final tiene que ver un poco con esa depuración, porque se tenían proyectos para adquirir licenciamiento de usuario final, pero el contrato Microsoft cambió el enfoque que se venía dando, no se realizó la inversión por que se estaría duplicando tecnologías y haciendo una inversión.

El Máster Rober Picado indica que comparte el tema de los recursos, señala que le dijo a Daniel que hay que sacar recursos para el proyecto y recursos para sostenibilidad, hoy por ejemplo se presentó el sistema de Planificación (NovaPlan) y se presenta una propuesta de recursos requeridos para cuando termine la implementación del sistema, acá se ve una buena planificación pensando en ir más allá, entonces se debería no solo pensar en los recursos para lo que falta del proyecto, si no considerar que si estamos implementando soluciones tecnológicas, también hay que presentar recursos para la sostenibilidad, sobre todo cuando se piensa en un personal tan pequeño como las unidades de seguridad.

El Ing. Daniel Berrocal indica que hay temas que se deben validar ya que cuando se estaba ejecutando este estudio se estaba dando la transición de que Don Robert estaba regresando a la DTIC, con base a las sesiones de coordinación que se han realizado, se está detallando todas las diferentes iniciativas, las tareas que tienen definidas cada una de ellas si tiene el cumplimiento al 100% o no, esto porque la fotografía en temas de ciberseguridad cambia de un día a otro, pueda ser que con una tecnología que estamos implementando, cumplimos algunos alcances que en su momento en el 2019 cuando se hizo esa hoja de ruta, no se tenía planificado que se pudiera realizar, a partir de ahí, se están analizando todas las que se puedan trasladar a la parte operativa, como la parte de capacitación o sensibilización, es una de las que se va a proponer pasar a la operativa ya que es un tema de mejora continua, además de eso se está detallando la cantidad de recurso humano que se va a necesitar para la parte de implementación, se detalla el plazo, y para la parte operativa para poderlo sostener se incluye el recurso humano.

El Ing. Leonardo Díaz, señala que en cuanto el Recurso Humano si bien se identificaron la necesidad de 12 recursos, el Plan de Reforzamiento también señala de un equipo intergerencial, donde no necesariamente estos recursos sean adquiridos nuevos, si no que en coordinación con las otras gerencias, tal y como se definió en el acuerdo 1 de la sesión del Consejo Tecnológico donde se vio el Plan Reforzado, hacer el análisis del recurso informático que pueden disponer que se dediquen únicamente en el desarrollo de las iniciativas del Plan de Ciberseguridad.

El Ing. Daniel Berrocal indica que él está recientemente en el puesto, por lo que refiriéndose de marzo a la fecha, indica que aunque no se haya logrado avanzar en todas las iniciativas, lo cierto es que se tienen algunos proyectos que son muy importantes y esenciales, que se ha logrado desarrollar en este periodo, que básicamente se puede mencionar el de seguridad perimetral, donde se atendieron una serie de actividades que estaban detallas en el Plan de Ciberseguridad, se logró la implementación del correlacionador de eventos, la implementación del SOC, que también atiende una de las iniciativas, se está adelantando lo de los contratos Microsoft para dar mayor seguridad en las terminales de usuario final, en esta línea, por lo menos este año, atreves de estos diferentes proyectos se están cerrando brechas de las que tienen definidas cada una de las diferentes iniciativas que componen este Plan de Ciberseguridad, hay temas que se deben mejorar como los controles, métricas entre otros, pero si aclarar que se están trabajando proyectos que van alineados con el Plan de Ciberseguridad.

El Ing. Erick Vindas agrega que hay que poner en contexto que se tuvo de por medio, desde la generación del Plan de Ciberseguridad, la pandemia y el ciberataque donde se tuvo la percepción de que muchas unidades como no tenían sistemas se dejaron de hacer actividades, sin embargo no fue el caso de Seguridad Informática donde se tuvo que trabajar para restablecer los servicios, aparte de eso considerar los cambios que se tuvo en el área de Seguridad y Calidad, y ahora con el trabajo realizado con Daniel y con Robert se ha efectuado ese ejercicio de hacer el desglose de tareas y actividades que están pendientes y que se puede ir integrando a la operativa diría, y como se comparte responsabilidades con el mismo negocio, por lo que es importante que se considere estos aspectos.

Respecto al hallazgo 8 el Máster Picado indica que este aspecto con el área de Ingeniería en Sistemas también lo vieron cuando se hizo el cruce entre el plan y presupuestos de los proyectos y el AGEDI, por lo que se señaló que se debe hacer la coordinación entre las áreas.

Respecto a las recomendaciones se atendieron las consultas respectivas y se realizaron los ajustes correspondientes según lo acordado en la sesión del comentario de informe.

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

LEONARDO FABIO DIAZ PORRAS (FIRMA)
Firmado digitalmente por LEONARDO FABIO DIAZ PORRAS (FIRMA)
Fecha: 2023.12.07 11:32:01 -06'00'

Ing. Leonardo Fabio Díaz Porras
Asistente de Auditoría

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2023.12.07 11:25:22 -06'00'

Ing. Rafael Ángel Herrera Mora, jefe
Área

RAHM/LDP/lbc

ANEXO 1
PRODUCTOS DE AUDITORÍA RELACIONADOS CON EL PLAN DE CIBERSEGURIDAD

Informe ATIC-68-2020 referente a la gestión integral del proyecto “Plan de Ciberseguridad de la CCSS”

De la evaluación realizada se extrae que:

- En cuanto a los requisitos previos para el desarrollo de la iniciativa “Plan de Ciberseguridad para la CCSS”, se identificó que no se encuentra implementado el prerrequisito “IMP02. Habilitación del Comité de Riesgos y Seguridad de la información”, el cual a su vez está supeditado a la ejecución de la propuesta “ITR03. Habilitar la estructura Organizacional de TIC”, las cuales se encuentran vinculadas de forma integral en el Modelo de Gobernanza de las TIC y de Seguridad de la Información.

- Se identificaron aspectos de mejora en torno al alcance del proyecto en cuanto a:

    - El procedimiento utilizado para establecer el alcance del proyecto donde se determine el tipo de lugares y aplicativos seleccionados en el alcance, así como las unidades y la cantidad de sitios a visitar por nivel de atención durante el desarrollo de la fase N°2 denominada “Análisis Actual”.
    - No se incluyó el equipo médico en ese apartado, el cual desde un ámbito integral de las TI representan dispositivos con software propietario interconectados a la infraestructura tecnológica institucional, por tanto, también se encuentran sujetos a riesgos de seguridad.
    - Se identificó falta de análisis en la situación actual de estos aparatos tecnológicos durante el desarrollo de la fase 2 “Análisis actual”, la cual va a determinar el contexto actual de ciberseguridad en la Caja Costarricense del Seguro Social para posteriormente, diseñar la hoja de ruta a seguir en aras de obtener el modelo deseado y las iniciativas a implementar.

- Se evidenció un atraso en el cumplimiento de las fechas establecidas en el cronograma de actividades para la ejecución de la Fase dos denominada *“Situación Actual”*, lo anterior debido a que se proyectó una duración de 4 meses para su desarrollo, sin embargo, se contabiliza un total de 11 meses desde su inicio en junio 2019 a mayo de 2020. Por consiguiente, producto de la situación descrita anteriormente, se afectó el tiempo de entrega de las fases tres, cuatro, cinco y seis, así como los plazos del subitem 1.1, por cuanto inicialmente se estableció en el cartel licitatorio y en el documento *“Plan Proyecto”* un término de entrega de 12 meses.

- Se determinaron oportunidades de mejora relacionadas con la estructura organizacional del componente denominado “Gestión del Cambio Organizacional”, lo anterior por cuanto solo se identifica la participación de funcionarios de 9 hospitales de un total de 29 en la Red de Agentes de Cambio, sin visualizar la representación de personal de Áreas de Salud, Sucursales, Direcciones de Redes Integradas de Prestación de Servicios de Salud, entre otros.

- Mediante la revisión documental de las minutas concernientes a la ejecución del Proyecto *“Servicios profesionales para desarrollar un Plan de Ciberseguridad para la CCSS”*, se determinó oportunidades de mejora por cuanto no se visualizó la definición de plazos para la atención de las tareas asignadas a los funcionarios a cargo, así como el seguimiento de las actividades establecidas en sesiones previas del equipo de trabajo que permita a la administración activa llevar un control y verificación del estado de cumplimiento.

Al respecto se emitió una recomendación dirigida a la Gerencia General, en la que se requirió de la elaboración de un plan remedial que valore elementos de gestión y proyecto que han incidido en su avance considerando los aspectos señalados en los hallazgos, asimismo, se dirigieron tres recomendaciones a la Dirección de Tecnologías y Comunicaciones, en torno a efectuar una revisión de los procedimientos utilizados para determinar la definición, justificación y selección del alcance del proyecto, así como una valoración en coordinación con las unidades que se estime pertinente, respecto a la inclusión del equipo médico dentro de esos aspectos, efectuar una valoración que determine la pertinencia de incluir mayor cantidad de funcionarios del ámbito local (Hospitales, Áreas de Salud, Sucursales, Direcciones de Redes Integradas de Prestación de Servicios de Salud, entre otros) así como valorar la inclusión de controles que permitan monitoreo de las actividades relacionadas con seguimiento y verificación del cumplimiento de los acuerdos efectuados a través de las minutas de las sesiones de los equipos de trabajo

AD-AATIC-063-2022 Oficio de Advertencia sobre Gobierno y Gestión de la Ciberseguridad en la CCSS.

- Se identificó la ausencia 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.

- 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.

- 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.

- 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. 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.

- Se mencionó la importancia de 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.

- Se concluyó 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 que 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.

- Respecto al proyecto de seguridad perimetral se indicó que 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.

- Sobre las fechas de inicio y avance de las iniciativas a desarrollar para subsanar brechas de Ciberseguridad, 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.

- 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, asimismo, 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.

- Teniendo en consideración el 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.
- Se indicó la importancia de que la administración ponga 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.

De lo anterior, la Auditoría previno y advirtió, de la situación planteada en el 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.

AS-AATIC-147-2022 Oficio de Asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social.

En dicho oficio de auditoría se denotó que:

- Se estima conveniente recordar la importancia de los roles y responsabilidades especializados en materia de seguridad de la información y ciberseguridad, los cuales fueron detallados 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”.

- Existen diferentes roles necesarios en una organización y de seguro irán saliendo nuevos cargos; por ello, es primordial incentivar la transformación de las estructuras tradicionales a las nuevas exigencias en ciberseguridad.

- Sin embargo, desde su reactivación por parte de la Junta Directiva en enero del 2018, el Consejo Tecnológico únicamente han sesionado dos veces al año, y durante el 2021, no se registra ninguna sesión, lo que representa a la fecha un periodo transcurrido superior al año desde la última reunión. Lo anterior adquiere relevancia si se considera el rol estratégico establecido a nivel del modelo de gobernanza y el manual de gestión respectivo aprobado por la Junta Directiva institucional donde se da a conocer la expectativa respecto de la función cumplir en el desarrollo de las tecnologías de información y comunicaciones en la CCSS.

- La política y procedimientos de una institución debe apoyar la definición del conjunto de elementos vinculados con la ciberseguridad, por lo que resulta de utilidad discurrir sobre las medidas por adoptarse en la CCSS, esto para tomar decisiones oportunas en la formación de cultura organizacional, por cuanto las normas, políticas y reglas son muy importantes porque establecen el direccionamiento dentro de la organización para personas, procesos y tecnologías; incentivándose la comprensión y el nivel de compromiso para cada uno de los actores involucrados en el proceso.

- Se debe impulsar desde los diferentes niveles organizacionales, el desarrollo y supervisión de iniciativas; involucramiento y capacitación de responsables; definición de funciones y actividades; vigilancia en el cumplimiento de plazos; y el análisis periódico de riesgos. Entre otras acciones, no menos importantes en la modernización de las estructuras, obtención de resultados y la adaptabilidad corporativa a la nueva realidad.

- La institución puede existir talento o destrezas para el liderazgo de iniciativas, los equipos de trabajo y conjunto involucrados, estos deben comprender ampliamente su participación en la generación de esfuerzos, aunado al desarrollo de capacidades que les permita garantizar el cumplimiento de objetivos, entre ellos, los correspondientes a impulsar la creación o reajuste de roles y responsabilidades en ciberseguridad.

- Debido a la complejidad que involucra el tema del ejercicio de roles y responsabilidades nuevos, se debe brindar seguimiento y supervisión a la atención de brechas y/o necesidades, en este caso particular, inmersas en el modelo de gobernanza TIC y seguridad de la información.

Al respecto, la Auditoría emitió la asesoría a la Administración, respecto a los roles y responsabilidades de ciberseguridad, con el propósito de ser sometidas a valoración y revisión por la Administración. Lo anterior, con el objetivo de enfrentar con éxito los eventos adversos que puedan presentarse, la mitigación de vulnerabilidades y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado de la ciberseguridad.

ANEXO 2
RECURSOS REQUERIDOS PARA LA IMPLEMENTACIÓN DE INICIATIVAS SEGÚN EL PLAN DE FORTALECIMIENTO DE CIBERSEGURIDAD

INICIATIVA	RECURSOS NECESARIOS
PCS-GI-01 Formalización de la implementación de la gestión del programa de ciberseguridad de la CCSS.	12 recursos de personal para la SSTI. Herramientas de Ofimática. Entes aprobadores del Nivel Jerárquico.
PCS-GI-02 Desarrollo y actualización de lineamientos y normativa que subsanen las brechas existentes.	12 recursos de personal para la SSTI. Herramientas de Ofimática. Entes aprobadores del Nivel Jerárquico.
PCS-GI-03 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.	12 recursos de personal para la SSTI. Herramientas de Ofimática. 1 recurso de personal para el seguimiento por parte de la Administración del sitio.
PCS-GI-04 Definición de los servicios de ciberseguridad que serán ofrecidos a través de la mesa de servicio de la CCSS.	12 recursos de personal para la SSTI. 2 recursos de personal para la SACI. Herramienta de software.
PCS-GI-05 Creación de un modelo de capacitación y especialización continua en Ciberseguridad y su integración con el Plan de Capacitación existente en la DTIC.	12 recursos de personal para la SSTI. Herramientas de software. Entes aprobadores del Nivel Jerárquico. Recursos Económicos de la DTIC.
PCS-GI-06 Desarrollo de una estrategia de respaldos institucional	12 recursos de personal para la SSTI. 12 recursos de personal para la AST. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Recursos Económicos de la DTIC. Áreas dueñas de los datos y servicios.
PCS-GI-07 Implementación de la gestión del riesgo cibernético	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios.
PCS-GI-08 Definición de una arquitectura de ciberseguridad que se alinee con los objetivos de la DTIC.	12 recursos de personal para la SSTI. 10 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios.
PCS-GI-09 Implementación de la gestión de vulnerabilidades y parches.	12 recursos de personal para la SSTI. 5 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.

INICIATIVA	RECURSOS NECESARIOS
PCS-GI-10 Implementar el Plan de Concientización en Ciberseguridad	12 recursos de personal para la SSTI. Herramientas de software para diseño. Entes aprobadores del Nivel Jerárquico.
PCS-GI-11 Implementación de la gestión de la seguridad de los endpoint.	12 recursos de personal para la SSTI. 5 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-12 Fortalecimiento de la identidad y gestión de acceso.	12 recursos de personal para la SSTI. 5 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-13 Gestión del acceso privilegiado en los sistemas de la CCSS.	12 recursos de personal para la SSTI. 5 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-14 Establecimiento e implementación de las líneas base de seguridad.	12 recursos de personal para la SSTI. Herramientas de Ofimática. Entes aprobadores del Nivel Jerárquico.
PCS-GI-15 Desarrollo del Centro de Operaciones de Seguridad (SOC) en la CCSS.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-16 Integración de la ciberseguridad a la metodología de desarrollo de software.	12 recursos de personal para la SSTI. 2 recursos de personal por Sistema de Información. Herramientas de Ofimática. Entes aprobadores de la DTIC.

PCS-GI-17 Simulación de ataques y pruebas de seguridad	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-18 Implementación de la gestión de la seguridad en la nube.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. Recursos Económicos de la DTIC.
PCS-GI-19 Implementación de la gestión de la seguridad con los proveedores de servicios.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios.
PCS-GI-20 Implementación del marco de cumplimiento en ciberseguridad y adopción de buenas prácticas.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios.
PCS-GI-21 Aprovechamiento de los acuerdos nacionales e internacionales para potenciar el conocimiento y desarrollo de la ciberseguridad en la CCSS.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios.
PCS-GI-22 Implementación de la privacidad y protección de datos en los servicios TIC.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios para Clasificar los datos. 1 CGI o informático local por sitio.
PCS-GI-23 Fortalecimiento de la seguridad perimetral.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. Recursos Económicos.
PCS-GI-24 Seguridad de Recursos Humanos.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Entes aprobadores del Nivel Jerárquico.

INICIATIVA	RECURSOS NECESARIOS
PCS-GI-25 Control de Acceso basado en Roles.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Áreas dueñas de los datos y servicios. Entes aprobadores del Nivel Jerárquico. 1 CGI o informático local por sitio.
PCS-GI-26 Gestión de Activos.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Áreas dueñas de los datos y servicios. Entes aprobadores del Nivel Jerárquico. 1 CGI o informático local por sitio.
PCS-GI-27 Seguridad de Sistemas.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Áreas dueñas de los datos y servicios. Entes aprobadores del Nivel Jerárquico. 1 CGI o informático local por sitio.
PCS-GI-28 Protección contra el Malwrare.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de software. Áreas dueñas de los datos y servicios. Entes aprobadores del Nivel Jerárquico. 1 CGI o informático local por sitio.
PCS-GI-29 Cifrado.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de software. Áreas dueñas de los datos y servicios. Entes aprobadores del Nivel Jerárquico. 1 CGI o informático local por sitio.
PCS-GI-30 Clasificación de la Información.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios para Clasificar los datos. 1 CGI o informático local por sitio.

INICIATIVA	RECURSOS NECESARIOS
PCS-GI-31 Pruebas de Penetración y Escaneo de Vulnerabilidades.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-32 Protección de la Marca.	12 recursos de personal para la SSTI. 2 recursos de la Dirección de Comunicación Organizacional. Entes aprobadores del Nivel Jerárquico.
PCS-GI-33 Analíticos y Operaciones de Ciberseguridad.	12 recursos de personal para la SSTI. 2 recursos de personal para cada Área de la DTIC. Herramientas de hardware y software. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Recursos Económicos.
PCS-GI-34 Respuesta de Incidentes.	12 recursos de personal para la SSTI. 5 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio.
PCS-GI-35 BCP Y DRP-Gestión de la Continuidad del Negocio y Estrategia de Recuperación.	12 recursos de personal para la SSTI. 12 recursos de personal para cada Área de la DTIC. Herramientas de ofimática. Entes aprobadores del Nivel Jerárquico. Áreas dueñas de los datos y servicios. 1 CGI o informático local por sitio. Sitio Alterno. Recursos Económicos de los sitios.

Fuente: Documento denominado "Plan de Fortalecimiento Proyecto de Ciberseguridad", noviembre, 2022.

ANEXO 3
RIESGOS Y/O LIMITACIONES IDENTIFICADAS POR INICIATIVA SEGÚN OFICIO GA-DTIC-3443-2023

Cód	Riesgos o limitaciones
PCS-GI-01	- Para la actividad No.2 descrita en la ficha técnica: Se requiere formalizar por parte de la DTIC desde el proyecto de Reestructuración y Gobernanza TI. GG-DTIC-1912022, mediante correo GG-DTIC-1910-2022 PCS-GI-01 aval Roles y Responsabilidades. - Para desarrollar la actividad No.3 descrita en la ficha técnica es necesario desarrollar la actividad No.2.
PCS-GI-02	- Es una de las iniciativas calificadas como de mejora inmediata para la continuidad exitosa y alineamiento del resto de los proyectos. - La ejecución del punto cuatro dependerá de avance o implementación de la propuesta de Gobernanza. - La evolución en el seguimiento de la aplicación de los lineamientos dependerá de la estructura organizacional de Gobernanza para la ciberseguridad que le brinde continuidad y ejecute los mecanismos de control interno que se van a crear, así como las responsabilidades, de lo contrario se deberá trasladar las tareas supra a las áreas de la DTIC existentes para el cumplimiento y evolutivo.
PCS-GI-03	- No se ha designado de manera formal al encargado por cada centro de gestión de informática. - Existen recomendaciones que están fuera del alcance del CGI.
PCS-GI-04	- Es una de las iniciativas calificadas como de mejora inmediata para la continuidad exitosa y alineamiento del resto de los proyectos. - La ejecución del punto cuatro dependerá de avance o implementación de la propuesta de Gobernanza. - La evolución en el seguimiento de la aplicación de los lineamientos dependerá de la estructura organizacional de Gobernanza para la ciberseguridad que le brinde continuidad y ejecute los mecanismos de control interno que se van a crear, así como las responsabilidades, de lo contrario se deberá trasladar las tareas supra a las áreas de la DTIC existentes para el cumplimiento y evolutivo.

PCS-GI-05	- Es necesario formular el modelo y trasladarlo a la DTIC para que sea contemplado dentro del plan de capacitación al ano correspondiente.
PCS-GI-06	- Depende de la ejecución de las iniciativas No. 2 y 5 - Desarrollo de iniciativa catalogado a Largo Plazo
PCS-GI-07	- Pendiente revisar la iniciativa de gobernanza - Buscar la Guia de valoración de Riesgos
PCS-GI-08	- Depende de la ejecución de las iniciativas No.2 y 5, así como del proyecto de Arquitectura Tecnológica de la CCSS - Desarrollo de iniciativa catalogado a Largo Plazo. - Se hace mención de la dependencia de un Modelo de arquitectura del cual se desconoce su existencia.
PCS-GI-09	- Hoy en día se está ejecutando la iniciativa con la empresa TECH CORE, aun así, hay que determinar si el punto 2 se va a realizar en conjunto con la empresa, dado que el resultado de la misma seria una compra. Existe un informe elaborado por PWC en donde se abarca temas sobre otras herramientas, no obstante, se debe analizar y actualizar. - Según registro de Vanessa Linea Base 23 iniciativas indica lo siguiente: "Se genera oficio a don Jorge Sibaja, consultando la estrategia de sustitución para el SCCM (respuesta 18 de abril 2022). Se desconoce si hay respuesta a este oficio", por lo tanto, se para el avance de la iniciativa se depende de la toma de decisión de otra unidad.
PCS-GI-10	- Depende de la ejecución de las iniciativas 2 - Desarrollo de iniciativa catalogado como Mejora Inmediata
PCS-GI-11	- Se considera prioritario tener una sesión con la comisión técnica la cual está a cargo de la elaboración de los documentos iniciales, y valorar si la compra abarca las actividades que están en los términos de referencia, compra "Soluciones para la Gestión de accesos, verificación de identidades y mitigación de vulnerabilidades". - Se necesita disponer de un inventario institucional para avanzar con la consecución de las demás actividades. - Analizar el informe PCS-ENT-040 Informe de herramientas para seguridad de los endpoints y determinar si va de la mano con la futura compra. - Valorar si dentro de los términos de referencia el alcance abarca la creación de Plan o simplemente es compra de licencias, tomar en cuenta que el plan lo puede desarrollar TECH CORE. - Es prioritario tener claro quién será el administrador de esta herramienta, ya sea por la estructura actual o bien bajo el nuevo modelo de Gobernanza.
PCS-GI-12	- No se tiene claro de cuantas contrataciones se está hablando. - ¿Si es una o más compras (soluciones) quien va a gestionar el proceso de adquisición y la ejecución del mismo? - Depende de la ejecución de las iniciativas 2 y 5. - Desarrollo de iniciativa catalogado como Mejora a corto plazo.
PCS-GI-13	- En el documento de Linea Base 23 iniciativas, se menciona en este punto los instructivos de: Proceso de clasificación de cuentas, generación y mantenimiento del inventario de cuentas privilegiadas. gestión de identidad privilegiados y sensibles, control de identidades sensibles. Es importante investigar la existencia de dichos instructivos. - Es prioritario tener claro quién será el administrador de esta herramienta, ya sea por la estructura actual o bien bajo el nuevo modelo de Gobernanza.

PCS-GI-14	- Depende de la ejecución de las iniciativas 2 y 5 - Desarrollo de iniciativa catalogado como Mejora a mediano plazo
PCS-GI-15	Actualmente la contratación del SOC se encuentra en el Área Jurídica, ya la comisión técnica hizo la recomendación. - Se está a la espera de que inicio el contrato. - Revisión periódica de las actividades realizadas por SOC y validación de potenciales oportunidades -
PCS-GI-16	- Depende de la ejecución de las iniciativas 2 y 5, también se debe analizar a nivel macro si se ocupa tener la 7 ya madura o en proceso con el tema de la gestión de ciber riesgos - La ficha indica que se debe tener apoyo de SICERE y Gerencia de Pensiones, no obstante se desconoce participación debido a que no se dispone de asesoría de PwC por cuanto el contrato ya finalizó. - Desarrollo de iniciativa catalogado como Mejora a corto plazo
PCS-GI-17	- Las herramientas que posee la empresa TECH CORE son Open Source y no son propiedad de la CCSS. - Se depende del contrato del SOC para la ejecución del plan de pruebas. - No se cuenta con personal en el SSTI para la ejecución de una simulación de ataques y su respectivo análisis. - A la fecha no se tiene establecido una capacitación la cual trate sobre los temas que abarcan la iniciativa 17. - No se dispone de un inventario de activos de la información críticos
PCS-GI-18	- Depende de la ejecución de las iniciativas 2 y 5, también se debe analizar a nivel macro si se ocupa tener la 7 ya madura o en proceso con el tema de la gestión de ciber riesgos - La ficha indica que se debe tener apoyo de SICERE y Gerencia de Pensiones, no obstante, se desconoce el criterio de la empresa PwC y no se dispone de asesoría debido que finalizó el contrato. - Desarrollo de iniciativa catalogado como Mejora a mediano plazo
PCS-GI-19	- Para la implementación de esta iniciativa es necesario que la gestión del riesgo cibernético este implementado.
PCS-GI-20	- Depende de la ejecución de las iniciativas 1,2,5. - Desarrollo de iniciativa catalogado como Mejora a corto plazo
PCS-GI-21	- El apoyo del Despacho de la DTIC es fundamental para el desarrollo de esta iniciativa
PCS-GI-22	- Tiene relación con la ejecución de varias iniciativas del proyecto de ciberseguridad, de gobierno de la seguridad de la información, implementación de la ley de protección de la persona frente al tratamiento de sus datos personales, proyecto de gobierno de datos, información institucional clasificada por los dueños del negocio, proyecto de gestión de activos TIC - Desarrollo de iniciativa catalogado como Mejora a mediano plazo - Según la ficha técnica se ocupa apoyo del despacho DTIC - Para hacer la compra de DLP es obligatorio catalogar todos los datos de la Institución y definir la prioridad (Seguridad de la Información)
PCS-GI-23	- Prerrequisitos de esta iniciativa corresponden a otras iniciativas que no han sido iniciado o se encuentran en proceso.