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

AS-AATIC-147-2022
19 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA- 2901

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA-1103

Licenciado
Luis Fernando Campos, gerente
GERENCIA ADMINISTRATIVA-1104

Doctor
Esteban Vega de la O, gerente
GERENCIA LOGÍSTICA-1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

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

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

Estimados(as) señores (as):

ASUNTO:	**Oficio de Asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y siendo consecuente a lo indicado en el oficio AI-874-2022 del 6 de junio del 2022 en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022, se asesora sobre los siguientes aspectos que refieren a los roles y responsabilidades en ciberseguridad a considerar en la Caja Costarricense del Seguro Social (CCSS).

1- ANTECEDENTES

1.1 Contexto actual de la ciberseguridad

La definición de ciberseguridad, también conocida como seguridad digital, es la práctica de proteger la información digital, dispositivos y activos de ataques maliciosos; ampliando dicho concepto la corporación de tecnología e informática, IBM, lo describe en el apartado "¿Que es la ciberseguridad?" publicado en su página web[1] de la siguiente manera:

> *"La ciberseguridad es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización."*

A ese respecto, la complejidad de este término involucra personas, procesos y tecnología, tal y como lo describe el proveedor tecnológico estadounidense de dispositivos para redes, CISCO, en su página web[2], citando:

> *"Un enfoque exitoso de ciberseguridad tiene múltiples capas de protección repartidas en las computadoras, redes, programas o datos que uno pretende mantener a salvo. En una organización, las personas, los procesos y la tecnología deben complementarse para crear una defensa eficaz contra los ciberataques. (…).*
>
> ***Personas:***
> *Los usuarios deben comprender y cumplir con los principios básicos de seguridad de datos, como elegir contraseñas seguras, ser cautelosos con los archivos adjuntos de los correos electrónicos y hacer copias de seguridad de datos. Obtenga más información sobre los principios básicos de ciberseguridad.*
> ***Procesos:***
> *Las organizaciones deben tener una estructura para manejar los ciberataques tentativos y sospechosos. Una estructura de buena reputación puede guiarlo y explicar*

[1] Enlace a página web: https://www.ibm.com/mx-es/topics/cybersecurity
[2] Enlace a página web, apartado de productos: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

cómo puede identificar ataques, proteger sistemas, detectar y responder a amenazas, y recuperarse de ataques exitosos. (…)
Tecnología:
La tecnología es esencial para brindar a las organizaciones y los individuos las herramientas de seguridad informática necesarias para protegerse de ciberataques. Se deben proteger tres entidades importantes: los dispositivos Endpoints (como computadoras, dispositivos inteligentes y routers), las redes y la nube. La tecnología común que se usa para proteger estas entidades incluye firewalls de próxima generación, filtrado de DNS, protección contra malware, software antivirus y soluciones de seguridad de correo electrónico."

Además, en esa misma publicación se cita la importancia de la ciberseguridad y quienes se benefician de ella, señalando:

"En el actual mundo conectado, todos se benefician de los programas de ciberdefensa avanzados. A nivel individual, un ataque a la ciberseguridad puede dar como resultado desde un robo de identidad hasta intentos de extorsión y la pérdida de datos importantes, como fotos familiares. Todos confían en las infraestructuras críticas, como las centrales eléctricas, los hospitales y las empresas de servicios financieros. Proteger estas y otras organizaciones es esencial para el funcionamiento de la sociedad.

Todos se benefician del trabajo de los investigadores de ciberamenazas, como el equipo de 250 investigadores de amenazas de Talos, que investiga las amenazas nuevas y emergentes y las estrategias de los ciberataques. Revelan nuevas vulnerabilidades, educan al público sobre la importancia de la ciberseguridad y refuerzan las herramientas de código abierto. Su trabajo hace que Internet sea más segura para todos."

Es decir, la labor supracitada en el ambiente laboral es responsabilidad de todos, esto desde la perspectiva de negocio y técnico, e incluyendo el nivel estratégico, táctico y operativo; tal y como lo menciona el artículo "La ciberseguridad es tarea de todos" publicado el 01 de febrero del 2019 por el proveedor de seguridad cibernetica Forcepoint, a saber:

"Estamos en un momento en el que procesamos una gran cantidad de información a través de la web. Desde la carga de documentos de interés general, hasta transacciones bancarias, mucho de nuestro día a día se desenvuelve ligado a distintas plataformas virtuales. Precisamente por eso, la ciberseguridad se ha convertido en un término de interés general que debe ser responsabilidad de todos.

Dentro de una empresa, la seguridad informática no debe ser tomada a la ligera. Existen distintos factores de ciberseguridad que pueden poner en riesgo la viabilidad de la información, desde el factor humano, hasta brechas o errores en códigos que afectan los procesos. Debido al avance de la tecnología, los sistemas de seguridad tradicionales ya no funcionan. Es por eso que a día de hoy se necesitan unos planes

de ciberseguridad dinámicos que se adapten a esos riesgos de la actualidad y que además puedan evolucionar de manera continua, mientras el negocio sigue creciendo."

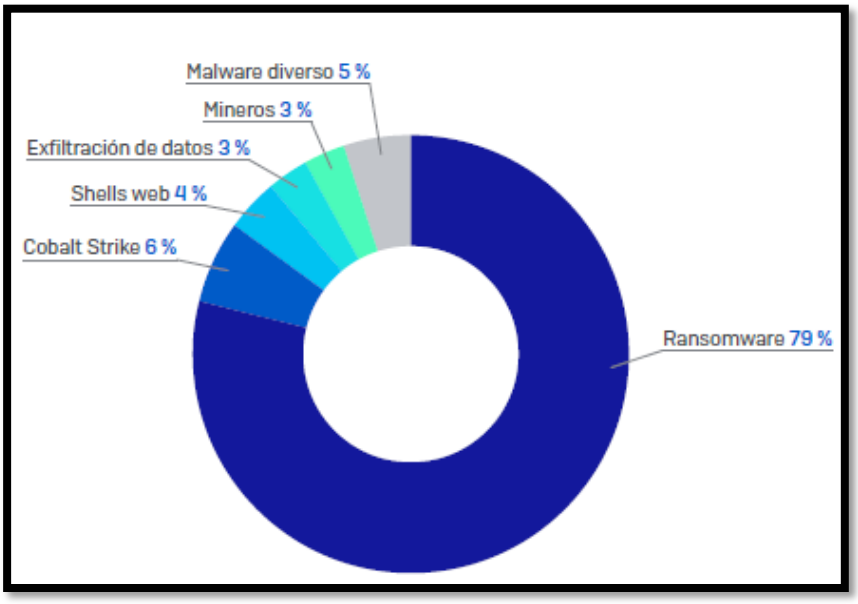
En virtud de lo anterior, surge el objetivo de alinear al conjunto de responsables en atender las necesidades crecientes en ciberseguridad, principalmente al considerar el incremento de ataques perpetrados alrededor del mundo, según revela la compañía "Accenture"[3] en su artículo "Tecnología Seguridad Estado de resiliencia en ciberseguridad 2021" publicado el 27 de enero del 2022, citando:

"Los ciberataques están en alza: Hubo una media de 270 ataques por empresa a lo largo del año, un aumento del 31% respecto al 2020. El riesgo de terceros sigue predominando: las infracciones efectivas a la organización por medio de la cadena de valor han aumentado de un 44% a un 61%.

Si observamos los resultados de la muestra efectuada en España, el incremento de los ciberataques fue de un 260% respecto a 2020. En cuanto al resto de porcentajes, la media en España se encuentra dentro del rango de resultados que muestra la encuesta global."

En ese sentido, en el periodo del 2020-2021 la empresa SOPHOS detalla en el "Informe de amenazas 2022" los incidentes atendidos por su equipo especializado, destacando:

Imagen No. 1
Sophos Rapid Response, motivo de las intervenciones de respuesta a incidentes durante 2020-2021



Fuente: "Informe de amenazas 2022", SOPHOS.

[3] Empresa multinacional de consultoría estratégica, servicios tecnológicos y externalización (outsourcing).

Como puede observarse, los delincuentes han creado ransomware para atacar a las organizaciones y están siendo más hábiles que la industria de la ciberseguridad al contrarrestar las amenazas cibernéticas.

Por ello, los especialistas han sido enfáticos al mencionar la necesidad de que las organizaciones inviertan en ciberseguridad (ajustes internos, equipamiento, software, recurso humano, entre otros recursos) debido a los efectos de los riesgos tecnológicos a los que se exponen.

Afirmando lo anterior, el articulo técnico de la revista "Securilatam" titulado "La inversión es estratégica para la resiliencia" del 01 de agosto del 2021, señala:

> *"Cuando nos consultan a la Fundación Capa8 sobre los desafíos de la ciberseguridad y la seguridad de la información, solemos explicar que el panorama es de un gran trabajo a desarrollar, con mucha concientización y con el deber de realizar un necesario nuevo ordenamiento de prioridades, acompañadas de inversión y generación de recursos humanos.*
>
> *Sabemos que las tareas de los encargados de proteger los activos cibernéticos no es nada fácil. En el caso de las empresas, como en los organismos públicos, se trata de un delicado equilibrio entre poder, tener y hacer.*
>
> *Si bien este comentario no necesariamente suele abarcar a todas las organizaciones, comprende a la gran mayoría de ellas. Sin discriminar tamaño ni ubicación geográfica, lo cual da origen a la cantidad de incidentes y ataques que se manifiestan a la fecha."*

Así las cosas, un ciberataque no solo supone una posible fuga de información, sino que pone en riesgo la operación de toda una institución, e inclusive en la prestación de servicios esenciales de todo un país, por ello el llamado a tomar las previsiones correspondientes.

1.2 Contexto de la CCSS en materia de ciberseguridad

La Caja Costarricense del Seguro Social (CCSS) no se encuentra exenta a la evolución de las Tecnologías de Información y Comunicaciones (TIC), ni al reforzamiento de los esquemas de seguridad de la información tradicionales.

De esa manera, en los siguientes apartados se detalla la estructura organizacional vigente de la Institución para abordar los temas de seguridad TIC; así como, las iniciativas que se mantienen en ejecución desde el 2017 para transformar el enfoque tradicional al especializado en ciberseguridad.

1.2.1 Estructura organizacional

La estructura organizativa de la Caja Costarricense de Seguro Social dispone de roles claves destinados a desempeñar labores en la definición y seguimiento de estrategias; toma de decisiones; ejecución de actividades dentro de las operaciones; así como otras funciones relacionadas con la gobernanza de las TIC y propiamente lo correspondiente a seguridad. En ese sentido, se detalla la identificación de perfiles funcionales en el tema de marras:

Consejo tecnológico

Este rol relevante en la generación de valor agregado para asegurar la gobernanza y gestión de las TIC y de la seguridad de la información, fue reactivado el 25 de enero de 2018, por la Junta Directiva en la sesión No. 8953, específicamente en el artículo N°28, al citar:

> *"Aprobar la reactivación del Consejo Tecnológico requerido para el Proyecto de Gobernanza de las TIC, el cual estará integrado por el Presidente Ejecutivo, los Gerentes, el Director de Tecnologías de Información y Comunicaciones y el Director de Planificación Institucional."*

En ese sentido, el "Manual Funcional del Consejo Tecnológico de la CCSS", octubre 2020, en su apartado 8.1 "Perfil funcional", refiere sobre la conceptualización del cuerpo colegiado, a saber:

> *"Es una instancia staff de alto nivel que busca habilitar la gobernanza en torno a las Tecnologías de la Información y Comunicaciones (TIC), estableciendo un espacio de dialogo y coordinación entre las gerencias de la institución y la Dirección de Tecnologías de Información y Comunicaciones (DTIC), con el fin de asegurar el apoyo de las TIC a la gestión y el cumplimiento de la estrategia institucional.*
>
> *Al estar integrado por las máximas autoridades de gobierno y administración de la Institución, junto con la Dirección de Tecnologías de la Información y Comunicaciones, y la Dirección de Planificación Institucional asume como cuerpo colegiado, la toma de decisiones sobre temas estratégicos asociados con las TIC que inciden en la prestación de los servicios a los usuarios."*

Además, en ese mismo marco normativo se define en el apartado 8.1.2, el objetivo general del Consejo Tecnológico de la CCSS, indicando:

> *"Hay que asegurar que la tecnología se convierta en una generadora de valor que apoye la ejecución de los procesos organizacionales y de los servicios que ofrece la Institución, y se encuentre en línea con la estrategia institucional, financiera y recursos de la Caja Costarricense de Seguro Social."*

Dirección de Tecnologías de Información y Comunicaciones (DTIC)

Según el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, aprobado por la Junta Directiva mediante el artículo No. 44 de la sesión No. 8555 de fecha 26 de enero de 2012), la DTIC es conceptualizada de la siguiente manera:

> *"**5.7.1 Nivel: Dirección***
> *Define los planes estratégicos políticas y directrices institucionales en su ámbito de competencia y lineamientos de tipo administrativo a nivel interno, formula, condensa y evalúa el Plan Operativo y el presupuesto, incluyendo la caja chica, administra los proyectos en tecnologías de información. Es responsable de conducir y coordinar las actividades de recursos humanos, con el propósito de lograr eficiencia, eficacia y productividad en la gestión.*
>
> *De acuerdo con lo definido por Junta Directiva, el Subdirector "… será responsable de la administración integral de los proyectos de tecnologías de información y comunicaciones, incluidos en el subportafolio de proyectos respectivo"*
>
> *Corresponderá a la Dirección de Tecnologías de Información y Comunicaciones decidir y autorizar qué unidad será la responsable del desarrollo de un sistema de información específico, conforme con el proceso establecido para la creación del portafolio y proyectos. El Consejo de Presidencia y de Gerentes y la Junta Directiva funcionarán como instancias de alzada, en caso de que así se requiera. (…)*
>
> ***Gestión Estratégica***
> *Es responsable de dirigir, planificar, coordinar, controlar y evaluar en forma estratégica los recursos y la gestión a nivel macro, con la finalidad de lograr el desarrollo efectivo de la organización, la oportunidad la calidad en la prestación de los servicios que se otorga a los usuarios y facilitar el cumplimiento de la misión y de la visión establecida."*

Dicha unidad tiene a su cargo cuatro áreas especializadas a nivel operativo, a saber:

- Área de Ingeniería en Sistemas.
- Áreas Comunicaciones y Redes Informáticas.
- Área Soporte Técnico.
- Área Seguridad y Calidad Informática.

Finalmente, es importante mencionar que la DTIC fue adscrita a la Gerencia General, según consta en el "Manual Organizacional Gerencia General", aprobado por la Junta Directiva de la Institución, en el artículo 8° de la Sesión N°8967 del 23 de abril de 2018 y en el artículo 3° de la Sesión N°8996 del 22 de octubre de 2018.

De esa manera, generándose valor agregado para posicionar el nivel de reporte de la DTIC en el Alto Jerarca de la CCSS; focalizando su atención en temas estratégicos, delegando la

operativa del día a día en los líderes de procesos tecnológicos y permitiéndole enfocarse en el seguimiento a iniciativas que buscan la mejora continua de servicios digitales.

En otras palabras, alineándose (al menos en su ubicación jerárquica) a las mejores prácticas que refieren a la gobernanza y gestión de las TIC y de la seguridad de la información.

Área Seguridad y Calidad Informática

En lo que refiere a roles y responsabilidades para el abordaje de la seguridad TIC en la Institución se identifica el Área de Seguridad y Calidad Informática, la cual realiza las siguientes funciones sustantivas, definidas en el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, aprobado por Junta Directiva, en el artículo No. 44 de la sesión No. 8555 de fecha 26 de enero de 2012:

> *"Es responsable de la seguridad y la calidad en el ámbito de las tecnologías de información y comunicaciones sí basándose primordialmente en que los sistemas de información desarrollados e implementados y la red institucional se administren en forma segura y confiable".*

En ese sentido, esa área depende jerárquicamente de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), y tiene a su cargó 3 subáreas, a saber:

- Subárea Seguridad en Tecnologías de Información.
- Subárea Continuidad de la Gestión.
- Subárea Aseguramiento de Calidad en Tecnologías de Información.

Centro de Gestión Informática

La estructura aplicable al Centro de Gestión Informática (en adelante CGI) se encuentra establecida en el Modelo de Organización de los CGI (octubre 2013), aprobado por la Junta Directiva en el artículo No. 44 de la sesión No. 8555 del 26 de enero de 2012 y artículo No. 32 de la sesión No. 8658 del 29 de agosto de 2013.

De acuerdo con dicho modelo de organización, el CGI es contextualizado de la siguiente manera:

> *"Es responsable de realizar las actividades operativas que apoyan el desarrollo de las tecnologías de información y comunicaciones, la ejecución de estudios de necesidades, la automatización de procesos estratégicos y operativos, participa activamente en la elaboración de planes, la administración de proyectos el desarrollo de los sistemas automatizados, implementa los mecanismos de coordinación, de comunicación, aplica las nuevas tecnologías, administra los equipos y las redes de información en su ámbito de competencia; es un enlace entre los usuarios no especializados, la Dirección de Tecnologías de Información y Comunicaciones y otros órganos competentes."*

Además, el documento identifica a los Centros de Gestión Informática como responsables del desarrollo operativo y la coordinación de actividades, en el nivel gerencial, regional y local; para tales efectos clasificándolos en dos niveles de complejidad:

- Modelo tipo A: Centros de Gestión Informática Gerenciales.
- Modelo tipo B: Centros de Gestión Informática Regionales y Locales.

Cada uno con su autoridad, cobertura y alcance, como se indica en el apartado 5.7 "Tipo y ámbito de autoridad" del marco normativo supra citado, a saber:

> *"Los Centros de Gestión Informática Gerenciales ejercen autoridad técnica-funcional en su ámbito de competencia, con las unidades que se encuentran adscritas a la gerencia correspondiente, mediante una amplia participación y trabajo en equipo.*
>
> *Los Centros de Gestión Informática Locales (Direcciones Regionales de Servicios de Salud y Sucursales, Hospitales Nacionales, Especializados, Regionales y Periféricos y las Áreas de Salud Tipo 3), ejercen autoridad técnica-funcional en su ámbito de competencia a las unidades que se encuentran adscritas, mediante una amplia participación y trabajo en equipo.*
>
> *La Dirección de Tecnologías de Información y Comunicaciones ejerce autoridad técnica sobre los Centros de Gestión Informática a nivel institucional."*

1.2.2 Marco Normativo

Con respecto al marco normativo interno, las Normas Institucionales en Tecnologías de Información y Comunicaciones, emitidas en abril del 2012, en el inciso 1.4 "Gestión de la seguridad de la información de TIC" menciona los niveles responsabilidad y otras consideraciones sobre el conjunto de reglas que aplican a la temática supra citada, citando:

> *"La Dirección de Tecnologías de Información y Comunicaciones a través del Área de Seguridad Informática será la encargada de emitir las Políticas Institucionales de Seguridad Informática y Normas Institucionales de Seguridad Informática, las cuales son de acatamiento obligatorio de todas las unidades de trabajo. A la vez, es la encargada de brindar la asesoría en cualquiera de los temas de seguridad informática."*

Particularmente, la Administración Activa mantiene vigentes la siguiente norma:

- Políticas Institucionales de Seguridad Informática, TIC-Seguridad-001, Versión 1.0 de octubre 2007.

  Sobre el particular, define en el inciso 5 del documento, el "Objetivo general de las políticas de seguridad informática", a saber:

"Brindar a las unidades y a los usuarios de tecnologías de información de la Caja Costarricense de Seguro Social, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos."

Seguido del inciso 6 "Objetivos específicos de las políticas de seguridad informática", citando:

"• Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para que los usuarios colaboren con la protección de la información y recursos institucionales.
• Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.
• Servir de guía para el comportamiento profesional y personal de los funcionarios de la CCSS, en procura de minimizar los incidentes de seguridad internos, como hurto de información o vandalismo.
• Promover las mejores prácticas de seguridad física, mediante la implementación de ambientes adecuados que permitan la correcta custodia de los datos y equipos administrados por los diferentes Centros de Gestión, utilización eficiente de los recursos de tecnologías de información.
• Regular el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.
• Homologar la forma de trabajo de personas de diferentes unidades y situaciones que tengan responsabilidades y tareas similares."

- Normas Institucionales de Seguridad Informática, TIC-ASC-SEG-0002, Versión 1.0 de abril 2008, las cuales son consideradas un complemento de las Políticas Institucionales de Seguridad Informática, tal y como lo indica el apartado 1 "Introducción" de dicho documento, a saber:

"Las Normas Institucionales de Seguridad Informática, son complemento del documento de Políticas Institucionales de Seguridad Informática, éstas son un conjunto de reglas que indican puntualmente lo que se debe hacer para cumplir con cada política. Según el diccionario de la Real Academia Española, norma se describe como:

"Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc."

Por lo anterior, además de detallar un conjunto de reglas o ajustes a las actividades relacionadas con el quehacer de los usuarios de las tecnologías de información, buscando la integridad, confidencialidad y disponibilidad de la información y recursos informáticos, se hace referencia a otros documentos como manuales o

procedimientos, que sirven de guía en el cumplimiento de lo estipulado en el presente documento.

Los estándares técnicos o de configuración, también constituyen normas, las mismas son una descripción de cómo la política de seguridad de la información será implementada, así como los mecanismos de seguridad asociados."

Finalmente, entre las consideraciones de regulación, las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado "Seguridad y Ciberseguridad", menciona la ruta en la que debe dirigir esfuerzos las instituciones, citando:

"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el

mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."

1.2.3 Iniciativa de la CCSS en materia de seguridad de la información y ciberseguridad

A través de los años la Institución ha conocido las brechas que refieren a necesidades en de ciberseguridad, tras evidenciarse datos alarmantes internos y externos sobre las múltiples amenazas cibernéticas y riesgos tecnológicos asociados al tema de marras.

Por ejemplo, Costa Rica se posiciona en el puesto No. 103 en el ranking de países atacados, lo anterior según los datos emitidos el 07 de julio del presente año por la empresa dedicada a la seguridad informática Kaspersky LAB o al observar el comportamiento de la cantidad de ataques cibernéticos detectados en la Caja, a saber:

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

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

Fuente: AD-AATIC-087-2022 del 16 de junio del 2022.

Sin dejar de lado, el incidente sufrido el pasado 31 de mayo, producto de un ciberataque que obligó (de manera preventiva) a desactivar todos los sistemas informáticos de la Institución; habiendo trascurrido hasta día de hoy, más de 40 días.

Así las cosas, las siguientes iniciativas (a través de dos licitaciones abreviadas) se han enfocado en diseñar un modelo meta, identificar brechas, establecer un plan de acción ante los hallazgos detectados, entre otros elementos no menos importantes.

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

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

Concretamente, entre los entregables de la Fase No.3 del proyecto de marras, el documento E3 denominado: "Diseño del modelo meta integral de gobernanza de las TIC y Seguridad de la Información", en el apartado 5.5 "Roles y responsabilidades de cara a la gestión de la seguridad de la información" propone estructuras organizativas, las cuales desempeñan una

figura clave en la definición de estrategias, toma de decisiones, y ejecución de actividades, todas en materia de ciberseguridad.

A ese respecto, el modelo propuesto de seguridad de la información incluye la presencia de habilitadores que figuran según los siguientes roles y/o puestos:

- Comité de Riesgos y Seguridad[4] (Conformado por representantes de Junta Directiva y algunos de los roles citados a continuación).
- Ejecutivo de Seguridad de la Información.
- Ejecutivo de Riesgo Institucional.
- Ejecutivo de Continuidad de Servicios.
- Director Actuarial.
- Dueños de Servicios y Procesos Institucionales.
- Gestor de Seguridad Informática.
- Custodios de activos de información.
- Usuarios de la Información.

Posteriormente, en el desarrollo de la Fase No.4, se entregó el documento E4 denominado: "Análisis integral de brechas", especificando a través de la tabla 50. "Identificación y análisis de brechas con respecto a las estructuras para la gobernanza de las TIC" y 51 "Identificación y análisis de brechas con respecto a las estructuras para la gobernanza de las TIC" el nivel de capacidad actual de la CCSS a partir de los hallazgos y brechas detalladas en el documento.

A ese respecto, se identificaron 13 hallazgos y 14 brechas relacionadas con las estructuras que habilitan la gobernanza y gestión de la seguridad de la información (véase Anexo 1 y 2 de esta misiva).

Por lo cual, en el entregable de la fase No. 5, visible en el documento E5 llamado "Plan de Acción consolidado para el cierre de brechas" de diciembre 2017, se establecieron dos iniciativas para abordar lo concerniente a la seguridad de la información, a saber:

Cuadro No. 2
Iniciativas Seguridad de la Información del
Modelo Meta de Gobierno de TIC y Seguridad de la Información, diciembre 2017-2022

Plazo definido	Iniciativa	Porcentaje de Avance a febrero 2022	Estado
Largo plazo	Implementar el Sistema de Gestión de Seguridad de la Información	0.00%	No iniciado
Mediano plazo	Establecer el Plan Táctico de CiberSeguridad	70.00%	Ejecución - En implementación

Fuente: Dirección de Tecnologías de Información y Comunicaciones, febrero 2022.

[4] Integrado por Representantes de Junta Directiva, Ejecutivo de Seguridad de la Información, Ejecutivo de Riesgo Institucional, Ejecutivo de Continuidad De Servicios, director Actuarial, Gestor de Seguridad Informática, Dueños de Servicios y Procesos Institucional Clave, Director de la Dirección de Tecnologías de Información y Comunicaciones.

Para tales efectos, la proyección de ejecución se indicó a 6 meses posterior a la finalización del Proyecto de Gobernanza, Gestión y Seguridad de la CCSS (iniciativas a corto plazo); las iniciativas de mediano plazo a 12 meses, específicamente considerando que deben estar implementados los prerrequisitos para su ejecución; y las acciones a realizar en el largo plazo requieren un alto nivel de madurez para ser implementadas, por lo cual su desarrollo es bajo las condiciones de orden y priorización de las actividades antes indicadas.

En ese sentido, es relevante mencionar que ya han trascurrido más de cuatro años desde el diseño del modelo meta, identificación de brechas y el establecimiento del plan de acción correspondiente.

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

En el 2019, la DTIC gestionó la Licitación Abreviada No. 2019LA-000001-1150 cuyo objeto contractual corresponde a "Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS" y constaba de la ejecución de seis fases[5]:

Particularmente, entre los entregables del proyecto de marras, se especifica la necesidad de disponer de roles y responsabilidades de ciberseguridad para toda la fuerza laboral e inclusive terceros interesados, así como su comprensión que debe existir sobre el tema (concientización y capacitación).

Además, reforzando la importancia del recurso humano especializado en el soporte organizacional inscrito a ciberseguridad, tal y como se cita en el apartado 7.1.6 del entregable de la Fase No. 5 denominado "Plan de Ciberseguridad, PCS-ENT-029", versión 1.0 de diciembre 2020.

> *"La ciberseguridad abarca un ecosistema interconectado de personas, procesos y tecnologías que requiere del alineamiento y el soporte de los Gerentes, la Junta Directiva y el negocio en general para poder proteger los elementos de mayor criticidad o "joyas de la corona". Por lo tanto, la seguridad de las TIC debe soportarse sobre el modelo meta de gobernanza de la seguridad de la información institucional, la cual oriente estratégicamente a la ciberseguridad, dicte las políticas, normativas y regulaciones aplicables a la CCSS de cara a la seguridad, habilite roles y responsabilidades en el negocio para poder suministrar los insumos requeridos a la ciberseguridad e identifique cuáles son los activos críticos que las TIC deberán soportar.*
>
> *Este soporte será clave para que la DTIC pueda habilitar la estrategia de ciberseguridad y articular los esfuerzos institucionales de cara a la visión futura de la ciberseguridad en la CCSS, lo cual constituye el principal reto y dependencia para*

[5] Según el documento PCS-ENT-001 "Plan Proyecto"

poder aumentar los niveles de madurez de la ciberseguridad hasta alcanzar el estado deseado para la Institución."

Finalmente, entre lo pertinente al entregable de la Fase No. 6, se define en el documento PCS-ENT-033 llamado "Roles y responsabilidades de ciberseguridad", la descripción para los siguientes perfiles profesionales:

- Gestor de ciberseguridad
- Arquitecto de ciberseguridad
- Técnico de monitoreo.
- Roles TIC con responsabilidades de ciberseguridad

En ese sentido, los insumos documentales trabajados por la institución describen a personas, procesos, tecnología, datos y ciberseguridad, necesarios para la puesta en marcha de una transformación digital.

2- OBSERVACIONES

Así las cosas, es importante para este Órgano Fiscalizador hacer un recordatorio a esa Administración sobre la relevancia que reviste el tema de roles y responsabilidades en ciberseguridad, máxime considerando los ataques cibernéticos reincidentes y reiterativos a las plataformas tecnológicas de la Institución.

En ese sentido, a través de las siguientes observaciones se hacen reseñas asociadas con el establecimiento de estructuras que apoyen la transformación digital de la Institución. Asimismo, cada apreciación debe ser evaluada y aplicarse según el mérito o impacto atinente al proceso objeto de mejora.

2.1 Sobre los roles inscritos a la práctica de ciberseguridad

Esta Auditoría Interna estima conveniente recordar la importancia de los roles y responsabilidades especializados en materia de seguridad de la información y ciberseguridad, los cuales fueron detallados anterioridad por la empresa consultora PWC en los entregables del proyecto de "Gobernanza TIC y Seguridad de la Información" y "Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS", compilados en el siguiente cuadro:

Cuadro No. 3
Identificación de roles clave diseño de modelo de Gobernanza TIC y Seguridad de la Información (2017) y Plan de Ciberseguridad para la CCSS (2020)

Rol	Descripción breve de la Responsabilidad
Comité de Riesgos y Seguridad	Este comité es el encargado de garantizar el adecuado seguimiento y revisión de los mecanismos implantados dentro de la CCSS para el aseguramiento de la información, evaluando, proponiendo y discutiendo las estrategias y prácticas

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

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

En ese sentido, las tendencias de gestionar requerimientos asociados con la especialización del recurso humano surgen ante la transformación digital y el rápido avance de los ciberataques; esto por medio de roles destinados a garantizar el adecuado direccionamiento

de los procesos, frente a determinadas amenazas que se proliferan en los sistemas e infraestructuras de negocio.

En ese orden de ideas, la especialización necesaria del personal que apoya las labores técnicas y de negocio hoy en día, se puede observar en la publicación dada a conocer por la compañía de asesoría profesional "Delfos Sistemas Informáticos" emitida el 27 de junio del 2022, titulada "Nuevos roles en ciberseguridad", a saber:

- CEO (Chief Executive Officer): Es el cargo más alto dentro del organigrama empresarial y es el responsable final de las acciones que se lleven a cabo en el negocio.
- CIO o jefe de sistemas: Actúa como responsable del área TI, encargado de planificar las estrategias tecnológicas del negocio.
- CTO (Chief Technology Officer): similar al CIO -es un puesto técnico- se encarga de que los sistemas de información funcionen de forma óptima.
- CISO (Chief Information Security Officer): la seguridad de la información está bajo su responsabilidad. Su principal función es garantizar la protección de los datos.
- CSO (chief sustainability officer): Es el responsable ejecutivo de la seguridad de la organización. Se encarga de mantener la seguridad de la empresa en general.
- Arquitecto de seguridad: Responsable de crear las estructuras de seguridad complejas y hacer que funcionen.
- Analista de ciberseguridad: Un perfil más técnico que tendría como misión principal la coordinación de la implementación de controles específicos de seguridad para cualquier sistema o servicio a incorporar en la empresa.
- Informático Forense: Como su propio nombre sugiere, va a recabar todo acerca de adquirir, preservar, obtener y presentar datos que hayan sido procesados y guardados en soportes digitales.
- Hacker (Ético): perfiles muy técnicos capaces de encontrar cualquier brecha, fisura o debilidad en un sistema… y comunicarlo, así como dar las posibles soluciones para eliminar esos riesgos.

Bajo ese contexto, 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.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información" , emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), al señalar en el Apartado XI, Seguridad y Ciberseguridad, lo siguiente:

> *"Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución."*

Aunado a valoraciones exhaustivas que aseguren un diseño, implementación y puesta en marcha del sistema de gestión de seguridad, acorde a las necesidades actuales y venideras de la Caja.

2.2 Políticas y procedimientos que apoyen los roles y responsabilidades en ciberseguridad

Complementario a la observación supracitada, la política y procedimientos de una institución debe apoyar la definición del conjunto de elementos vinculados con la ciberseguridad. De este modo, siendo consecuente con lo indicado en "Las Normas técnicas para la gestión y el control de las Tecnologías de Información" emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), al señalar en el Apartado XI, Seguridad y Ciberseguridad, lo siguiente:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados."*

Caso contrario, podría materializasen riesgos, tales como los mencionados en el artículo "Expertos urgen la creación de un marco regulatorio de ciberseguridad en México" publicado el 6 de octubre del 2021, por parte de "Yahoo! Finanzas"6, a saber:

> *"De acuerdo con el estudio de Metabase Q, México tiene un alarmante el rezago en cuanto a regulación sobre ciberseguridad; no solo respecto al resto de los países, sino a los desafíos en la materia.*
>
> *Lo que hace a México un blanco para los ataques cibernéticos es:*
>
> *-La falta de un marco regulatorio sólido e innovador.*
> *-La falta de programas en ciberseguridad efectivos (defensa y resiliencia cibernética).*
> *-Una baja cultura de concientización sobre la importancia de la ciberseguridad.*
>
> *(…) El estudio de Metabase Q establece que la ciberseguridad debe verse como una prioridad en la agenda pública. A su vez, hace hincapié en que es importante desarrollar una infraestructura institucional que atienda el tema; sin embargo, para ello se debe contar con un marco regulatorio sólido e innovador que esté a la altura de los desafíos del ecosistema digital.*

[6] Yahoo! Finanzas es un servicio del Navegador Web Yahoo! que proporciona información financiera y comentarios con un enfoque en los mercados de América del Norte.

(…) De acuerdo con los expertos, más allá de la falta de un marco regulatorio sólido, uno de los principales problemas del México en materia de ciberseguridad radica en la falta de cultura y concientización de los ciudadanos mexicanos frente a esta.

«Existe esta falsa percepción de que la ciberseguridad es un tema que solo debe regularlo el gobierno o que es un tema que solo atañe al sector privado y muy enfocado a las empresas que formamos parte de las tecnologías de la información y no hay nada más falso que eso», dice Servín."

Aunque la publicación refiere al contexto actual de México y su marco normativo de ciberseguridad, resulta de utilidad discurrir sobre las medidas por adoptarse en la CCSS, esto para tomar decisiones oportunas en la formación de cultura organizacional.

En ese sentido, la determinación de 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.

2.3 Adaptabilidad de la organización para atender las necesidades en ciberseguridad

Las organizaciones de la actualidad, sin importar su dimensión deben trabajar en la mitigación del riesgo para garantizar la sostenibilidad de las operaciones y al mismo tiempo prepararse ante las disrupciones tecnológicas. En ese sentido, la adaptabilidad al cambio aporta valor a la toma de decisiones, generación de oportunidades y consecuentemente la previsión de amenazas o requerimientos en el negocio.

Según establecen "Las Normas técnicas para la gestión y el control de las Tecnologías de Información" emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), al señalar en el Apartado III, "Planificación Tecnológica Institucional", al señalar:

"La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público.

Adicionalmente, que incorpore indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia."

A ese respecto, la revista española "Cuadernos de Seguridad" publicó el 10 de junio del 2022, el artículo "En ING, el empleado es un colaborador muy importante en materia de seguridad", refiriéndose a retos de adaptabilidad organizacional, citando:

"Actualmente nos enfrentamos al gran reto de adaptarnos constantemente a un entorno muy cambiante en el que tenemos que abordar la ciberseguridad como un todo y sin perder el foco en la innovación. Desde la irrupción de la pandemia, se ha intensificado el uso de dispositivos móviles, las herramientas de colaboración y el acceso en remoto; y esto también nos ha llevado a nuevos riesgos y ciberamenazas para las que tenemos que estar preparados. Por ello, como CISO es fundamental tener un punto de vista integral de la ciberseguridad, abarcando procesos y objetivos de negocio, analizando los riesgos TIC y poniendo en marcha soluciones innovadoras que se puedan integrar desde el punto de vista de la monitorización, así como de la prevención del fraude."

En otras palabras, las organizaciones deben estar en sintonía con la evolución de las tecnologías en aras de mitigar amenazas, disminuir brechas, y reorganizar los recursos; lo cual implica cambios estructurales, tecnológicos, de productos o servicios y culturales.

Parte de esas modificaciones son la creación de nuevos roles y responsabilidades para abordar la realidad respecto a la ciberseguridad; no obstante, esa premisa debe evitar la materialización de riesgos como los mencionados en el artículo "Los 10 errores de gestión de vulnerabilidades que siguen cometiendo los CISO" de la revista española "CSO Computerworld" publicado el 16 de junio del 2022:

*"**1. No conseguir el respaldo de los ejecutivos***

(…) los CISO necesitan el apoyo de múltiples actores en la organización para hacer bien esta tarea, y es más probable que obtengan ese apoyo cuando tienen el respaldo de los líderes más altos dentro de la empresa, dice Michael Gray, CTO del proveedor de servicios gestionados Thrive.

Por otro lado, los CISO que carecen de apoyo a nivel ejecutivo para sus esfuerzos de gestión de la vulnerabilidad pueden verse obstaculizados por la falta de claridad sobre el riesgo aceptable y la resistencia de las unidades de TI y de negocio (…)

2. No fomentar la responsabilidad compartida

"Los CISO cargan con la responsabilidad o el riesgo de la gestión de vulnerabilidades: no deberían", dice Alex Attumalil, CISO de Under Armour.

Los CISO no son dueños de los sistemas o de las funciones de negocio que apoyan, ni tienen la autoridad para determinar únicamente si la organización se siente cómoda aceptando algún riesgo en particular."

Por todo lo anterior, 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.

2.4 Desarrollo de capacidades

Con el objetivo de garantizar razonablemente el éxito de las estrategias o iniciativas asociadas a la generación de roles en ciberseguridad, las recomendaciones de estándares de calidad, conocidos como "ISO"; marcos de referencia especializados; guías de mejores prácticas; tendencia de la industria y el marco normativo; aluden a el despliegue de esfuerzos planificados para gestionar el cambio y concientizar a toda la organización sobre las pretensiones organizacionales.

Particularmente, desarrollando capacidades para afrontar los cambios de paradigmas, propiciar el aprovechamiento de recursos, mejorar la comunicación, así como otras labores de apoyo para el desarrollo de actividades, que en su mayoría poseen niveles de complejidad altos y por ende deben ser sistematizadas cuidadosamente.

Lo anterior, según lo señala las Normas de Control Interno para el Sector Público, en su apartado 1.2 al describir los "Objetivos del SCI":

> *"El SCI de cada organización debe coadyuvar al cumplimiento de los siguientes objetivos:*
>
> *(…) c.* ***Garantizar eficiencia y eficacia de las operaciones****. El SCI debe coadyuvar a que la organización utilice sus recursos de manera óptima, y a que sus operaciones contribuyan con el logro de los objetivos institucionales."*

Un ejemplo de la verificación de capacidades es citado en el artículo "El nuevo rol de los CIO y CTO" de la revista estadounidense "Entrepreneur" compartido el 25 de abril del 2022, a saber:

> *Las empresas de hoy deben darse cuenta del papel cambiante de la tecnología en sus operaciones. Luego, deben considerar si sus líderes tecnológicos tienen el mandato, el equipo y la autoridad adecuados para desempeñarse de manera óptima."*

Por otra parte, el artículo "Siete estrategias para construir un equipo de seguridad fuerte" de la revista española "CSO Computerworld" publicado el 3 de enero del 2022, señala la importancia de habilitar capacidades para los equipos de trabajo y recursos para el desempeño de labores, mencionando lo siguiente:

> *"El experto en ciberseguridad y CISO de servicios al cliente de Oracle, Brennan P. Baybeck, cree que una de sus primeras responsabilidades es la construcción de un equipo humano con éxito. "Si te rodeas de gente excelente, asegúrate de que tengan lo que necesitan, como programas de capacitación o buenos presupuestos. De este modo se consiguen altas cotas de ciberseguridad", dice. Este enfoque requiere muchos recursos de desarrollo, así como planificación y dirección de carrera para que*

los miembros puedan desarrollar mejor sus habilidades y tengan la combinación correcta de responsabilidades. Sin estos ingredientes, la seguridad sufre.

"Un equipo insatisfecho derivará en luchas internas, infelicidad y agresiones", asegura un informe de la consultora Forrester. "Esto no solo cultivará un entorno desagradable, sino que también tiene el potencial de arruinar la reputación del departamento, socavar su integridad y poner en riesgo a toda la organización" (…)"

Otro aspecto por mencionar es la concientización integral, sabiendo que educar a todos los participantes sobre las metas, inversiones, cambios estructurales, entre otros aspectos. Lo cual genera valor agregado, a la capacidad de juicio y responsabilidad, tal y como se indica en la nota del 3 de marzo del 2022, titulada "Los directivos deben tener un mayor compromiso con la ciberseguridad" publicada por la revista digital española "itTrends", al citar:

"La seguridad cibernética está acaparando la atención a raíz del aumento de ataques de ransomware y otras amenazas que están causando estragos entre las empresas. Para hacer frente a estos problemas muchas organizaciones están aumentando el gasto en ciberseguridad, pero en muchos casos no se está adoptando un enfoque adecuado. Según un estudio realizado por los expertos en seguridad de Trend Micro, más del 90% de los responsables de la toma de decisiones empresariales y de TI están muy preocupados por los ataques de ransomware.

Pero muchos directivos y administradores de TI no se muestran lo suficientemente comprometidos con la seguridad. Una muestra es que solo un 57% de los equipos de TI encuestados debaten sobre los riesgos cibernéticos con los directivos, con una periodicidad semanal, como poco. Eva Chen, CEO de Trend Micro, explica que "las vulnerabilidades solían pasar meses o incluso años antes de ser explotadas tras su descubrimiento".

Pero ahora el panorama ha cambiado, y los ciberdelincuentes aprovechan muchas vulnerabilidades de seguridad en tan solo unas horas desde que se descubren. Según Chen, "más ejecutivos que nunca entienden que tienen la responsabilidad de estar informados, pero a menudo se sienten abrumados por lo rápido que evoluciona el panorama de la ciberseguridad". Por ello, afirma que los responsables de TI necesitan una mejor comunicación con los directivos de su organización, de forma que puedan entender con más claridad los grandes riesgos a los que están expuestos y mitigarlos lo antes posible.

La parte positiva es que la inversión en ciberseguridad no está descendiendo, ya que un 42% de los encuestados afirma que su organización es la que más gasta en reducir el riesgo empresarial. Por debajo quedan otras áreas, como la transformación digital (36%) y la transformación de la plantilla (27%). Y un 49% dice que su organización ha aumentado la inversión para reducir los riesgos derivados del ransomware y las brechas de seguridad.

El problema, según los expertos, es que la falta de conocimiento y concienciación de los directivos con la ciberseguridad conduce a inversiones mal enfocadas, lo que dificulta adoptar estrategias efectivas y genera más riesgos financieros. Y solo un 46% de los encuestados afirma que su organización tiene un amplio conocimiento de conceptos como el ciber riesgo o la gestión del ciber riesgo. Un 77% de las empresas quiere responsabilizar a más personas de la gestión y la mitigación de estos riesgos, pero solo un 38% incluye en este grupo a los CEO. Asimismo, solo un 28% quiere implicar más en esta materia a los CFO y un 22% a los CMO."

Si bien es cierto, en 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.

2.5 Seguimiento y supervisión de requerimientos asociados con roles y responsabilidades

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.

Lo anterior, en apego a las Normas de Control Interno para el Sector Público, en su apartado 4.5.1 "supervisión constante", al señalar:

"El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos."

Además, en el apartado 4.5.2 "Gestión de proyectos" de ese mismo marco normativo, 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:

a) *La identificación de cada proyecto, con indicación de su nombre, sus objetivos y metas, recursos y las fechas de inicio y de terminación.*

b) *La designación de un responsable del proyecto con competencias idóneas para que ejecute las labores de planear, organizar, dirigir, controlar y documentar el proyecto.*

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.*

En ese sentido, resaltando el rol y la participación del Consejo Tecnológico, de forma continua para evitar la materialización de riesgos asociados a la desarticulación de esfuerzos e inversiones; limitaciones en la toma de decisiones oportunas para la aprobación, inicio y seguimiento de proyectos estratégicos con componentes tecnológicos; la ausencia de monitoreo y detección de desviaciones durante su desarrollo; así como el incumplimiento de las responsabilidades establecidas en el cuerpo normativo.

De lo contrario, podría estarse enfrentando la Institución a conflictos como los mencionados en el artículo "¿Quién es responsable de la ciberseguridad y privacidad?" publicado en enero del 2021, por el proveedor tecnológico a nivel mundial "Kingston Technology", al citar:

> *"(…) los altos directivos siguen sin tomarse en serio la ciberseguridad y la privacidad de los datos. Con demasiada frecuencia consideran que estas tareas pueden delegarse al director de Seguridad de la Información (DSI/CISO) o al responsable de protección de Datos, y que eso es todo. Si la alta dirección sigue viendo las cosas de esta manera, no es de sorprender que esta actitud trascienda a los niveles inferiores de las organizaciones, y que en ninguno de los estamentos se tomen en serio estas cuestiones."*

Por tanto, dadas las responsabilidades delegadas al Consejo Tecnológico, su labor podría evitar barreras que pongan en riesgo la vigencia de los entregables generados en cada una de las etapas, cambio del personal; reprocesos por modificaciones internas o normativas; disposición de recursos financieros; cambios de prioridades; trasformaciones en otras estructuras organizacionales interrelacionadas; entre otros obstáculos que podrían inhibir o retrasar la implementación de proyectos.

3- CONSIDERACIONES FINALES

La Caja Costarricense del Seguro Social, dentro de su gestión y servicios que presta a la población depende de las Tecnologías de Información y Comunicaciones, las cuales para su buen desempeño deben tener claramente definidos sus roles, responsabilidades y autoridades para responder a situaciones específicas.

Sobre el particular, haciendo énfasis a lo correspondiente en ciberseguridad, aspecto que incluye normativa, políticas, tipificación de recursos, procesos, entre otros elementos garantes de la estructura organizacional; segregación de tareas; definición de cargos; rectoría; términos y condiciones.

Todo lo anterior, bajo el contexto de ciberataques en alza, la necesaria transformación digital y demás elementos que enfrenta la Institución en cada uno de los procesos de salud, pensiones y recaudación patronal, se debe planificar la puesta en marcha de una estrategia en ciberseguridad, sin omitir lo atinente a los roles y responsabilidades afines a esa práctica.

Por ello, se considera relevante la participación y empoderamiento del Consejo Tecnológico, en la premisa de generar de valor agregado para asegurar la gobernanza y gestión de las TIC y de la seguridad de la información, donde se incluyen cierre brechas e iniciativas asociadas con el ejercicio de roles y responsabilidades en seguridad de la información y ciberseguridad. En otras palabras, la alta dirección debe tomar conciencia y liderazgo en priorizar y dar seguimiento a los proyectos que pretenden aumentar las capacidades a la CCSS.

Así las cosas, ese accionar busca asegurar que los roles, responsabilidades y autoridades sean claros para el sistema de gestión de seguridad y a partir de ello, las partes interesadas (entre ellas la DTIC y unidades a cargo) desplieguen lo correspondiente a nivel estratégico, táctico y operativo para adaptarse a las necesidades del negocio, bajo el ordenamiento de prioridades y la articulación de esfuerzos.

Además, reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI, al construir una estructura con roles y responsabilidades acorde a las perspectivas de ciberseguridad y/o disposición de: normas actualizadas; evaluación de riesgos; capacidades y recursos; cultura organizacional; conciencia y compromiso; medición del desempeño y rendición de cuentas; entre otros factores que propician la implementación de controles y madurez en un esquema de ciberdefensa.

De conformidad con expuesto en el artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones ejecutadas, resulta fundamental que la Administración Activa se mantenga vigilante en la adopción de acciones pertinentes y suficientes en el tema de marras.

Asimismo, es importante que las acciones ejecutadas incluyan los mecanismos básicos de control que aseguren la legalidad de las operaciones y a su vez acrediten documentalmente

los lineamientos y directrices considerados para dirigir adecuadamente la gestión de negocio y TI.

En virtud de lo expuesto, se da conocer las observaciones insertas en el oficio, con el propósito de ser sometidas a valoración y revisión por esa 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.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.19 16:11:05 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

Anexos (2)

1. Identificación y análisis de brechas con respecto a las estructuras para la gobernanza de las TIC en la CCSS, 2017.
2. Identificación y análisis de brechas con respecto a las estructuras para la gestión de las TIC en la CCSS, 2017.

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva-1102
Licenciado Mayid Morales Madrigal, director, Proyecto Reestructuración Organizacional del Nivel Central-2918.
Auditoría.

Anexo 1
Identificación y análisis de brechas con respecto a las estructuras para la gobernanza de las TIC en la CCSS, 2017

Rol	Hallazgos	Brechas identificadas
Comité de Riesgos y Seguridad	La gestión de riesgos de TIC, así como la seguridad de la información se visualizan como responsabilidad exclusiva de las áreas de TIC; por lo que no existe el involucramiento y corresponsabilidad requerido por parte de las gerencias y áreas de negocio de la Institución.	Habilitar como parte del proceso institucional de riesgos, un Comité de Riesgos y Seguridad la Información, que dicte las políticas, el plan de gestión y brinde seguimiento en materia de riesgos tecnológicos y seguridad de la información.
		Este comité debe contar con representación de Seguridad de la Información, Riesgo Corporativo, Continuidad de Servicios, Seguridad Informática, Dueños de servicios y procesos institucionales clave y Tecnologías de Información y Comunicaciones.
		Establecer las políticas de funcionamiento del Comité y establecer claramente sus responsabilidades.
	El comité de riesgos existente está enfocado en la Gerencia de Pensiones y la gestión de riesgos de inversiones.	

Fuente: Elaboración propia, a partir de la información contenida en la tabla 50. "Identificación y análisis de brechas con respecto a las estructuras para la gobernanza de las TIC del documento E4 denominado: "Análisis integral de brechas"

Anexo 2
Identificación y análisis de brechas con respecto a las estructuras para la gestión de las TIC en la CCSS, 2017

Rol	Hallazgos	Brechas identificadas
Ejecutivo de Seguridad de la Información	No existen roles que se hagan responsables de liderar iniciativas de alcance institucional sobre aseguramiento, privacidad y disponibilidad de la información, y que alineen las mismas a la operativa de la CCSS.	Establecer una función centralizada responsable de la administración de la seguridad de la información nivel institucional.
	La gestión de seguridad de TIC se visualiza como responsabilidad exclusiva de las áreas de TIC; por lo que no existe el involucramiento y corresponsabilidad por parte de las gerencias y áreas de negocio de la Institución.	Establecer una figura que se encargue de definir el alcance del sistema de gestión de la seguridad de la información, establecerlo y darle el mantenimiento el garantice la mejora continua del mismo y el acoplamiento adecuado con los cambios organizacionales.
		Habilitar un rol de apoyo a la gestión de riesgos institucional, que garantice que dentro de la misma se incorpora la planificación para el tratamiento de los riesgos sobre la seguridad de la información.
Ejecutivo de Riesgo Institucional	No existe un rol responsable de liderar la gestión de riesgos de las operaciones y servicios de la CCSS, que habilite los mecanismos que permitan asegurar que los riesgos son identificados y gestionados en todos los giros organizacionales.	Establecer una función centralizada responsable de la administración de la gestión de riesgos a nivel institucional.
	La gestión de los riesgos de TIC se visualiza como responsabilidad exclusiva de las áreas de TIC; por lo que no existe el involucramiento y corresponsabilidad por parte de las gerencias y áreas de negocio de la Institución.	Habilitar un rol de apoyo a la Alta Gerencia, que le brinde el asesoramiento y retroalimentación adecuada y oportuna sobre las estrategias definidas para el tratamiento de los riesgos a nivel institucional.

Rol	Hallazgos	Brechas identificadas
Ejecutivo de Continuidad de Servicios	La gestión de la continuidad de TIC se visualiza como responsabilidad exclusiva de las áreas de TIC; por lo que no existe el involucramiento y corresponsabilidad por parte de las gerencias y áreas de negocio de la Institución.	Establecer una función centralizada responsable de la administración de la continuidad de los servicios y las operaciones a nivel institucional.
	No existen figuras responsables de habilitar y liderar la continuidad de las operaciones y servicios de la CCSS, que garantice que los mecanismos implantados para la continuidad de la CCSS se apegan a los estándares definidos y se alinean con la gestión financiera, de riesgo y de seguridad.	Establecer un rol que defina una estrategia de continuidad institucional ante situaciones adversas, y aborde su implementación y mejora continua.
		Habilitar un rol de garantice el alineamiento de la gestión de continuidad con la gestión de riesgos y la gestión de seguridad de la información.
Dueños de Servicios y Procesos Institucionales	Existen figuras responsables de habilitar la prestación de los servicios de la CCSS, sin embargo, un mismo servicio dentro de la CCSS puede tener varias figuras que fungen como propietarias en diferentes unidades institucionales, dificultando la estandarización en procesos y prácticas.	Habilitar figuras por giros de servicios y procesos institucionales y locales que apoyen en la implantación de un sistema de gestión de la seguridad de la información.
	No existe claridad sobre cuáles procesos y servicios son de ámbito institucional o de ámbito local.	Contar con roles con conocimiento y empoderados de los servicios y procesos institucionales, capaces de brindar guía sobre los puntos sensibles y críticos relacionados con la información.
	El conocimiento sobre procesos y servicios institucionales está distribuido en múltiples figuras cuya visión de estos se enfoca en el ámbito laboral donde se desenvuelven.	
Custodios de activos de información	El resguardo y la ejecución de procedimientos para el aseguramiento y disponibilidad de la de la información, se delega únicamente a las unidades TIC; por lo que no existe el involucramiento y corresponsabilidad por parte de las gerencias y áreas de negocio de la Institución.	Habilitar figuras por área de servicio responsables de los activos de información sensibles, en medios físicos o tecnológicos que garantice el resguardo y adecuado funcionamiento de los activos de información.
	Las unidades de prestación de servicios institucionales, tales como hospitales y centros de salud, no poseen figuras que garanticen que los procedimientos de seguridad, disponibilidad y privacidad de los expedientes y documentación sean los adecuados.	

Fuente: Elaboración propia, a partir de la información contenida en la tabla 51 “Identificación y análisis de brechas con respecto a las estructuras para la gestión de las TIC” del documento E4 denominado: “Análisis integral de brechas”