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

AD-ATIC-046-2022
3 de mayo de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100.

Máster
Roberto Blanco Topping, subgerente a.i

Máster
Mayra Ulate Rodriguez, jefe
Área de Seguridad y Calidad Informática
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Estimado(a) señores(a):

ASUNTO:	**Oficio de Advertencia referente a la priorización de la ciberseguridad 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, esta Auditoría advierte sobre aspectos relacionados con la priorización de la ciberseguridad en la Caja Costarricense del Seguro Social.

Lo anterior, considerando el aumento exponencial y malintencionado de ciberataques en Costa Rica y que ha sido dirigido a determinadas plataformas tecnológicas con vulnerabilidades en sus sistemas de información.

En ese sentido, la situación antes indicada ha significado un impacto negativo en la reputación o funcionamiento de las TIC[1] e inclusive de las organizaciones.

Por tanto, la CCSS no fue exenta de esos ciberataques e inclusive debe permanecer alerta y consciente de la necesidad inminente de propiciar un ambiente seguro y controlado que le permita gestionar de manera eficiente y responsable la exposición a amenazas de fraude, uso inadecuado de datos, pérdida o robo de información, entre otros.

Según lo establecen 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”, a saber:

> ***“XI. SEGURIDAD Y CIBERSEGURIDAD***
>
> *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.*

[1] Las Tecnologías de la Información y las Comunicaciones (TIC) / Tecnologías de la Información (TI)

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. ANTECEDENTES

1.1 Ciberataques recientes en Costa Rica

El país se ha mantenido recientemente en el blanco de los ciber atacantes, según lo confirman los eventos comunicados por los periódicos diarios, donde informan una afectación originada por infecciones de ransomware[2], sustracción de información sensible y otras afecciones a portales, sistemas y bases de datos de instituciones públicas y empresas del sector privado, entre ellas la Caja Costarricense del Seguro Social (CCSS).

Tal y como lo resume la nota del 26 de abril del 2022 publicada por el diario nacional El Financiero, titulada "*Conti ataca dos instituciones más: Inder y la Sede Interuniversitaria de Alajuela*", en la cual cita las organizaciones vulneradas, a saber:

"El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) confirmó que el grupo de hackers Conti atacó dos nuevas instituciones, la Sede Interuniversitaria de Alajuela y el Instituto de Desarrollo Rural (Inder).

(…) A la fecha hay entidades atacadas: los ministerios de Hacienda, Ciencia y Trabajo, el Fondo de Desarrollo Social y Asignaciones Familiares (Fodesaf), el Instituto Meteorológico Nacional (IMN), Radiográfica Costarricense S. A. (Racsa), Caja Costarricense del Seguro Social (CCSS) y Junta Administrativa del Servicio Eléctrico Municipal de Cartago (Jasec).

[2] El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

También la empresa Aeropost, alertó sobre un incidente que atacó al proveedor del sistema que gestiona la información de sus clientes de sus nueve sedes y específicamente de las tarjetas de crédito, lo que sería una situación independiente de la crisis en Costa Rica."

No obstante, Costa Rica habitualmente se ha mantenido expuesta a numerosos intentos de ciberataques que no se han materializado o no son dados a conocer públicamente, según detalla la nota periodística emitida por el periódico "La República" el pasado 11 de febrero, titulando "Costa Rica experimentó más de 2.500 millones de intentos de ciberataques en 2021", detallando:

"Costa Rica experimentó más de 2.500 millones de intentos de ciberataques en 2021, según datos de Fortinet, empresa mundial de soluciones de ciberseguridad.

Según datos recabados por FortiGuard Labs, el laboratorio de inteligencia de amenazas de Fortinet, México fue el país latinoamericano que más intentos de ataques recibió con 156 mil millones, seguido de Brasil con 88,5 mil millones, Perú con 11,5 mil millones y Colombia con 11,2 mil millones.

El reporte de 2021 revela que los países de América Latina y el Caribe se encuentran a la par de otras regiones y han sido objetivo de cerca del 10% del total de intentos de ciberataques que se han dado el último año en el mundo."

1.2 Estrategia de Gobierno para fortalecer las medidas de ciberseguridad del sector público

En línea con lo anterior, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT) anunció la directriz N° 133- MP-MICITT, con el objetivo de instruir a la Administración Pública Central e insta a la Administración Pública Descentralizada a cumplir una serie de medidas frente a los ciberataques que afecta al país y probablemente persistentes en el futuro.

En ese sentido, la norma entró en vigor a partir del 21 de abril del 2022 y pretende facilitar y agilizar la articulación de procesos de atención y prevención de incidentes informáticos en pro del fortalecimiento de la ciberseguridad del país.

Con la directriz, las instituciones deben acatar las recomendaciones y medidas técnicas que formule el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), a través de la Dirección de Gobernanza Digital y el CSIRT-CR, quien funge como ente coordinador de la ciberseguridad nacional.

1.3 Implementación de políticas y estrategias de seguridad TIC en la CCSS

El marco normativo interno vigente a nivel institucional consiste en los siguientes documentos:

- Políticas Institucionales de Seguridad Informática, TIC-Seguridad-001, Versión 1.0 de octubre 2007
- Normas Institucionales de Seguridad Informática, TIC-ASC-SEG-0002, Versión 1.0 de abril 2008.

Sin embargo, ambos documentos citados contemplan únicamente conceptos propios del contexto en el cual fueron desarrollados; principalmente asociados con la seguridad informática y no así de ciberseguridad, debido a que han trascurrido más de 14 años desde su elaboración.

En ese sentido, la Administración al considerar el entorno de las TIC en comparación a las recomendaciones dadas por las mejores prácticas a nivel de la industria; las necesidades tecnológicas actuales; las tendencias tecnológicas y los retos a futuro de innovación y mejora continua, propone generar una contratación asociada con la implementación de un modelo de gobernanza tanto en TI como en seguridad de la información.

Bajo ese contexto, la Dirección de Tecnologías de Información y Comunicaciones (DTIC) tramitó la licitación abreviada No. 2016LA- 000003-1150 “Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS”, con el fin de convenir con la consultoría el apoyo en la obtención de un modelo de gobernanza en tecnologías de información y en seguridad de la información.

Por consiguiente, la contratación fue adjudicada mediante el oficio GIT-4505-2016 del 22 de setiembre del 2016, a la empresa Price Waterhouse Coopers Consultores S.A. (PwC), por un monto máximo de ₡373,600,000.00 (Trescientos setenta y tres millones seiscientos mil colones con 00/100), firmándose el contrato No. 007-2026, al cual se le otorgó la aprobación interna mediante oficio DJ- 06772-2016 emitido por la Direccion Jurídica el 14 de noviembre del 2016. Es decir, con esta contratación dio inicio el 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 el 16 de enero del 2017.

Por tanto, las condiciones contractuales establecen el cumplimiento de fases y entregables para disponer del modelo meta, con fundamento en etapas de planificación del proyecto, comprender el contexto del negocio, definir el modelo meta integral, analizar las brechas, definir el plan de acción para el cierre de brechas y definir un plan de intervención.

Particularmente, el entregable de la Fase 4 “Analizar las brechas integrales del Gobierno de las Tecnologías de Información y Comunicaciones evaluando el Gobierno de la Seguridad de la Información”, diagnosticó el ambiente institucional en ese momento y afirma la necesidad de orientar la operación y función de las TIC, hacia una perspectiva de gobierno y gestión TIC, así como de la gobernanza de la seguridad de la información.

En ese mismo entregable, el apartado 5.5 “Análisis del Modelo de Gestión de Seguridad de la Información”, del Informe Diseño del modelo meta integral de gobernanza de la TIC y Seguridad de la Información, refiere **sobre la visión estratégica**, los siguientes hallazgos clave:

- No existen iniciativas institucionales impulsadas por la Alta Direccion que permitan consolidar un modelo de gestión de seguridad de la información.
- Existe un entendimiento asociado a la seguridad de la información que se centra únicamente en el aseguramiento de la soluciones y plataformas tecnológicas, caracterizado por la delegación de responsabilidad sobre la seguridad a las unidades de TIC, por lo que no existe el involucramiento y corresponsabilidad por parte de los usuarios.

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

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

Bajo esas condiciones, la empresa contratada plantea la definición de roles que puedan comprender y resolver las brechas supracitados, entre ellos los siguientes:

- Comité de Riesgos y Seguridad, para el caso de la Gobernanza.
- Ejecutivo de la Seguridad de la Información.
- Ejecutivo de Riesgo Institucional.
- Ejecutivo de continuidad de Servicios.
- Dueños de servicios y procesos institución.

- Custodios de activos de la información.

En ese mismo informe, también se realizó un análisis de los **estándares aplicables a la seguridad de la información** desde la perspectiva de ISO 27001, identificando, hallazgos y brechas en la Institución, señalando entre otros, los siguientes:

- No hay una conciencia clara a nivel institucional sobre la relevancia de la información para el desarrollo de los servicios y operaciones institucionales, lo cual imposibilita identificar el nivel de impacto que sufriría la CCSS ante la materialización de incidentes sobre la información.
- No existen principios ni lineamientos institucionales oficiales sobre la seguridad de la información.
- No existe un seguimiento que garantice la efectividad de los controles de aseguramiento de la información implementados.
- No existen procesos formales de uso institucional que habiliten la gestión de riesgos relacionados a la seguridad de la información.
- No existe una definición y asignación clara de roles y responsabilidades que soporte la gestión institucional de la seguridad de la información.
- No existen medidas y procedimientos sancionatorios definidos e implementados para los funcionarios que incurran en violaciones a la seguridad o privacidad de la información o hagan incurrir a la institución en incidentes de seguridad.

Posteriormente, se tramitó la Licitación Pública No. 2019LN-000001-1150 Servicios Profesionales de Consultoría para el acompañamiento en la implementación del Modelo de Gobernanza y Gestión de las TIC en la CCSS, el cual fue adjudicada mediante oficio GG-1678-2019 del 23 de octubre de 2019 por el Dr. Roberto Cervantes Barrantes, Gerente General, a la firma Price Waterhouse Coopers y la contratación 2019LA-000001-1150 “Servicios profesionales para desarrollar el Plan de Ciberseguridad para la CCSS”, la cual fue adjudicada el 16 de febrero de 2019, a la empresa Price Waterhouse Coopers Consultores S.R.L. y se firmó el contrato No. 010-2019.

Lo anterior, con el fin de continuar brindando apoyo a la Institución en las siguientes iniciativas (véase Tabla 1) relacionadas con la ciberseguridad, así como su nivel de avance desde su conceptualización hasta la fecha, a saber:

Tabla 1
Estado de avance de Proyectos al 13 de octubre del 2021

Nombre de la iniciativa	Diseño	Implementación
Habilitar la gestión de operaciones de tecnologías de información y comunicaciones desde la perspectiva de las seguridades operativas.	0%	0%
Establecer el plan táctico de ciberseguridad	100%	10%
Habilitación del comité de riesgos y seguridad de la información	0%	0%
Implementar el sistema de gestión de seguridad de la información	0%	0%

Fuente: Informe de diagnóstico programa de Gobernanza de las TIC (PGTIC) GG-EAN-001-2021 del 26 de noviembre de 2021.

Como se puede observar las iniciativas citadas anteriormente y conceptualizadas a partir de los entregables del PwC transmitidos el 2017, aún se encuentran en proceso de ejecución, particularmente en las etapas de diseño e implementación, sin embargo, de maneral general el porcentaje de avance es bajo en relación con el tiempo trascurrido, la cantidad de labores asociadas a cada proyecto y los requerimientos de la CCSS en esta materia.

1.4 Productos emitidos por la Auditoría Interna

Si bien es cierto la Caja ha formulado acciones relacionadas al tema, este Ente de Control y Fiscalizador ha sido insistente en diferentes momentos para señalar a la Administración las oportunidades de mejora relacionadas con la disponibilidad de estrategias avanzadas de ciberseguridad y prevención del fraude.

Por ejemplo, la temática antes indicada ha sido señalada con anterioridad mediante los siguientes productos:

Cuadro No.1
Productos emitidos Auditoría Interna sobre Seguridad de la TIC y ciberseguridad

Informe / Oficio No.	Fecha	Asunto
Informe de Auditoría ATIC-049-2014	09 de mayo de 2014	Gestión de la seguridad de la información institucional y el rol que cumple el Área de Seguridad y Calidad informática.
Informe de Auditoría ATIC-127-2015	15 de junio de 2015	Avance en proyectos de adquisición e implementación de software y hardware de seguridad informática.
Informe de Auditoría ATIC-45-2016	4 de abril de 2016	Fortalecimiento de la infraestructura de seguridad en Tecnologías de Información y Comunicaciones.
Oficio 47886-2017	14 de febrero de 2017	Oficio Informativo respecto al marco normativo relacionado con la Privacidad y Confidencialidad de la Información en las Comunicaciones.
Informe de Auditoría ATIC-72-2017	9 de agosto de 2017	Avance del proyecto modelo de gobernanza de las tecnologías de información y comunicaciones y de seguridad de la información de la Caja Costarricense de Seguro Social (CCSS).
Oficio 53581-2017	22 de agosto de 2017	Observaciones relacionadas con la Seguridad Informática de la Información de los servicios institucionales de Tecnologías de Información y Comunicaciones (TIC) accesados a través de dispositivos móviles.
Oficio 53708-2017	6 de septiembre de 2017	Aspectos relacionados a la Seguridad Informática de acuerdo con temas abordados en el Convenio de Ciberdelincuencia celebrado en Budapest.
Informe de Auditoría ATIC-106-2017	29 de septiembre de 2017	Gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de una contratación directa de servicios profesionales a la Firma Consultora Deloitte & Touche.
Oficio 6441-2018	13 de abril de 2018	Observaciones relacionadas con el Gobierno de Seguridad de la Información.
Informe de Auditoría ATIC-83-2018	23 de julio de 2018	Cumplimiento de la Ley No. 8968 “Protección de la Persona Frente al Tratamiento de sus Datos Personales” y su reglamento en la Caja Costarricense de Seguro Social (CCSS).
Oficio AD–ATIC–8137–2018	24 de septiembre de 2018	Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS.
Oficio No. 9125	8 de octubre de 2018	Resultado informe denominado “Evaluación de carácter especial sobre la gestión efectuada en el cumplimiento de los planes remediales del Análisis Integral de Vulnerabilidades y Riesgos en TIC de la CCSS.
Oficio No. 11069	20 de diciembre de 2018	Oficio de información sobre aspectos relacionados con la Seguridad de la Información Institucional”. (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema).
Informe de Auditoría ATIC-246-2018	21 de diciembre de 2018	Gestión de la Gerencia de Pensiones en el cumplimiento a las Normas de Seguridad Informática Institucional.
Oficio AI-2328-2019	9 de agosto de 2019	Dispositivos móviles institucionales.
Oficio AD-ATIC-271-2020	5 de febrero de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
Oficio 292	15 de febrero de 2019	Aspectos relacionados con seguridad de la información. (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema)
Oficio AD-ATIC-706-2020	16 de marzo, 2020	Continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre del 2019
AD-ATIC-896-2020	22 de abril de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1239-2020	20 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).

Informe / Oficio No.	Fecha	Asunto
AD-ATIC-1322-2020	25 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1512-2020	29 junio de 2020	Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio.
AS-ASTIC-1849-2020	23 de julio del 2022	Oficio de asesoría respecto a la seguridad cibernética (ciberseguridad) ante la pandemia producida por el COVID-19.
AS-ATIC-2062-2020	13 de agosto del 2020	Oficio de asesoría respecto al uso de VPN en la CCSS.
AI-202-2021	28 de enero del 2021	Oficio que refiere a los resultados de una revisión sobre el tema de "Amenazas de Correo Electrónico", con el objetivo de fortalecer el uso del correo electrónico bajo los principios de eficiencia, eficacia, ordenamiento jurídico y técnico.
AI-573-2021	11 de marzo del 2021	Oficio respecto a vulnerabilidad en Microsoft Exchange Server
AI-608-2021	15 de marzo del 2021	Oficio en el cual se emiten recomendaciones ante la exposición al ataque cibernético denominado "Solar Winds"
AS-ATIC-674-2021	24 de marzo del 2021	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2021 y preparación tecnológica de la CCSS
AD-ATIC-1806-2021	26 de agosto del 2021	Oficio de Advertencia referente a evento presentado respecto de la visualización de imágenes médicas en el Hospital Nacional de Niños.
AD-ATIC-1930-2021	9 de setiembre del 2021	Oficio de Asesoría referente a la Gobernanza de Tecnologías de Información y Comunicaciones (TIC) y Seguridad de la Información en la Caja Costarricense de Seguro Social.
AS-ATIC-2298-2021	1 de noviembre del 2021	Oficio de Asesoría respecto a los tipos de amenazas que afectan a las organizaciones por medio del accionar de los ciberdelincuentes.
AS-ATIC-2313-2021	1 de noviembre del 2021	Oficio de Asesoría referente a mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas.
AS-ATIC-2503-2021	30 de noviembre del 2021	Oficio de asesoría respecto a la preparación de los sistemas de información para la prevención al fraude.
AS- ATIC-052-2022	8 de abril del 2022	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2022 y preparación tecnológica de la CCSS
AD-ATIC-038-2022	21 de abril del 2022	Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo de 2022.
AD-ATIC-039-2022	21 de abril del 2022	Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS

Fuente: elaboración propia.

2. OBSERVACIONES

A continuación, se presentan observaciones relacionadas con la ciberseguridad en la institución y que a criterio de la Auditoría, la Administración debe revisar en el contexto actual para determinar la priorización necesaria en el abordaje del tema:

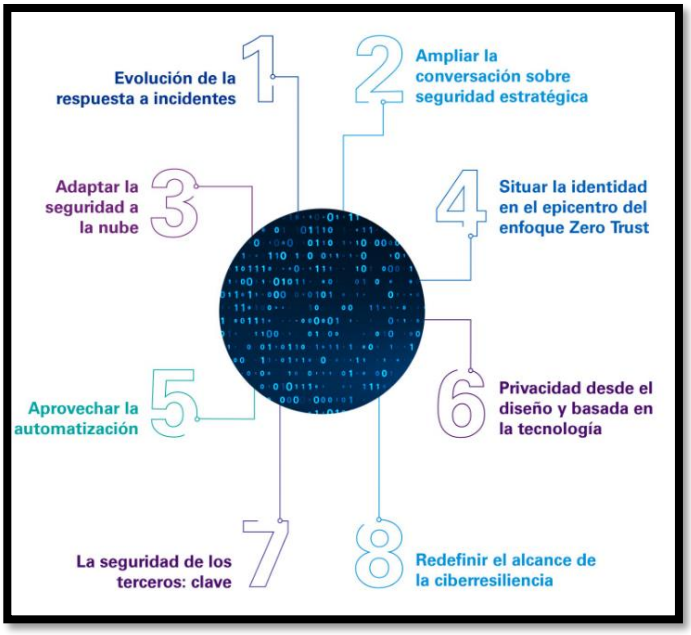
2.1 Sobre las medidas a implementar en la CCSS

Ante el conjunto de amenazas concretas derivadas del uso malicioso de las tecnologías digitales para lesionar la integridad de las organizaciones, el avance pausado de la CCSS en iniciativas relacionadas con la ciberseguridad correspondientes al "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", el marco normativo interno desactualizado y el deber de respuesta ante Incidentes de Seguridad Informática, la Institución debe considerar reforzar las actividades vinculadas con:

- Velar por el cumplimiento políticas, normas, protocolos y/o directrices asociadas a la ciberseguridad.
- Adaptar las estrategias vigentes de la organización al contexto actual de riesgo y/o robustecer el entorno asociado a la ciberseguridad.
- Establecer o corroborar las líneas de comunicación con los niveles técnicos y/o equipos de trabajo especializados.
- Prepararse con anticipación para la eventual puesta en marcha de planes de contingencia TI, así como los atinentes a la continuidad de los servicios tecnológicos y del negocio, para cuando suceda un eventual incidente.
- Verificar la estrategia del servicio en relación con los procesos de gestión de incidentes y/o problemas TI.
- Detección y análisis de manera continua y priorizada ante incidentes de ciberseguridad.
- Los responsables de detectar o resolver los incidentes de ciberseguridad deben mantener informados a los diferentes involucrados en los procesos tecnológicos y de negocio para que estos realicen el seguimiento, monitoreo o eventualmente brindar colaboración y apoyo en la resolución de situaciones extemporáneas.
- Proyectar y gestionar inversión en seguridad para responder de forma ágil ante incidentes.
- Motivar la solicitud de requerimientos técnicos que les permita hacer frente a actos asociados al robo y trasiego de datos.

En línea con lo anterior, KPMG (red global de firmas que presta servicios de Auditoría, Impuestos y Asesoría) propone valorar los aspectos visibles en la siguiente imagen, para incorporarlos en la estrategia de ciberseguridad de cualquier organización, a saber:

Imagen N°1
Ocho consideraciones para la estrategia de ciberseguridad de las empresas



Fuente: KPMG Tendencias, artículo "Ocho consideraciones para la estrategia de ciberseguridad de las empresas". marzo del 2022.

Ante ese escenario, adquiere relevancia definir de manera correcta la estrategia para definir la gestión de riesgos y preparar a la Institución de cara al futuro, considerando los elementos expuestos en la imagen, así como los indicados en nuestro oficio de advertencia AD-ATIC-039-2022, del 21 de abril del 2022, sobre la exposición a ataques cibernéticos a la CCSS, en el cual se generan observaciones mancomunadas con la temática de marras.

2.2 Sobre el fortalecimiento de los planes diseñados en materia de ciberseguridad

El modelo meta de gobernanza y gestión de las TIC y gobernanza de la Seguridad de la Información, fue diseñado en el 2017 por los especialistas de PwC consultando el marco de referencia ISO 27000[3] para lo correspondiente a temas de seguridad (Según el entregable 3 - Diseño del modelo meta integral de gobernanza de las TIC y Seguridad de la Información).

No obstante, a fecha ha trascurrido más de 4 años y podrían existir variaciones en conceptos o definiciones; nuevas tendencias; entre otros aspectos que puedan generar recomendaciones de valor agregado al proyecto citado anteriormente.

Un ejemplo de ello es el marco de ciberseguridad NIST (acrónimo de Instituto Nacional de estándares y tecnología, en inglés), el cual se centra en ayudar a las organizaciones en comprender, administrar y reducir sus riesgos TIC para proteger sus redes y datos. En ese sentido, se comparte una breve reseña de la información asociada al Framework, con el objetivo de que los datos sean objeto de análisis e investigación, a saber:

El marco supracitado da un abordaje integral de la ciberseguridad debido a que su estrategia es brindar un abordaje simple de la gobernanza de la ciberseguridad, permitiendo trasladar fácilmente conceptos técnicos a los objetivos y necesidades del negocio. Inclusive este marco de referencia al desarrollarse se basó en una variedad de estándares, entre ellos la ISO 27001, por lo cual no afectaría el diseño adquirido por la CCSS para gestionar la gobernanza de la seguridad.

Inicialmente, se debe percibir los siguientes enunciados que caracterizan al marco de ciberseguridad NIST:

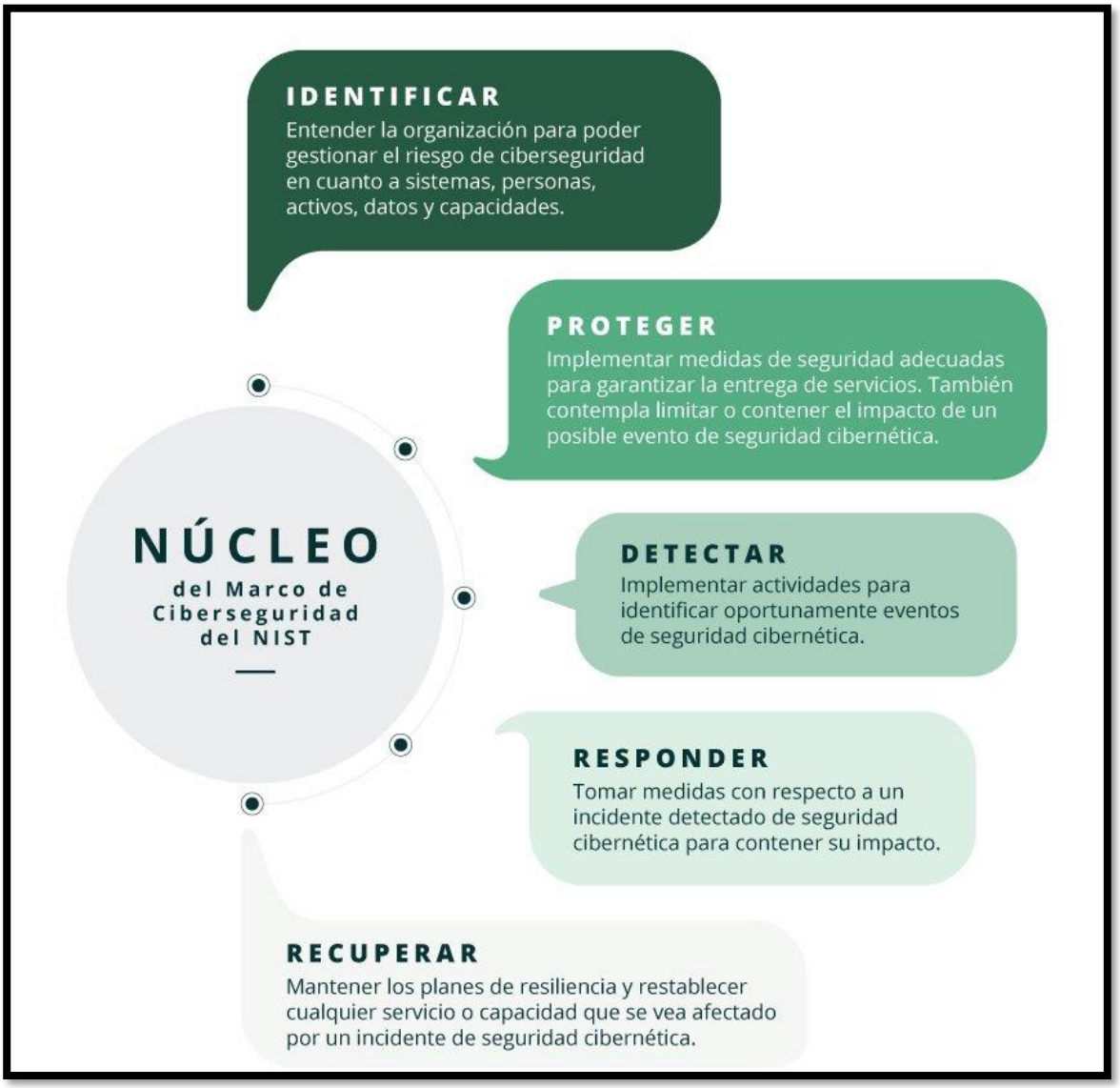
- Es aplicable para organizaciones de todos los tamaños y sectores.
- Conceptualmente fue diseñado para infraestructura crítica[4] de las organizaciones, pero debido a su versatilidad es posible implementarlo en los diferentes procesos tecnológicos.
- Su principal objetivo es reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por 3 partes:

    1. Núcleo del marco.
    2. Niveles de implementación.
    3. Perfiles del marco.

    En línea con lo anterior el núcleo del marco consta de 5 funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar. Para tales efectos, se puede apreciar en la siguiente imagen la representación de la estructura mencionada, así como una breve descripción de estas:

[3] La Organización Internacional de Estandarización (ISO, por sus siglas en inglés) estableció la norma ISO 27001, que se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales.
[4] La infraestructura crítica se define como: Sistemas y activos, ya sean físicos o virtuales, tan vitales que la incapacidad o destrucción de tales sistemas y/o activos tendría un impacto debilitador sobre la seguridad nacional, la económica nacional o la salud pública, o cualquier combinación interrelacionada a estos asuntos.

Imagen N°2
Núcleo del marco de referencia NIST



Fuente: Marco Ciberseguridad del NIST, extraído de piranirisk.com

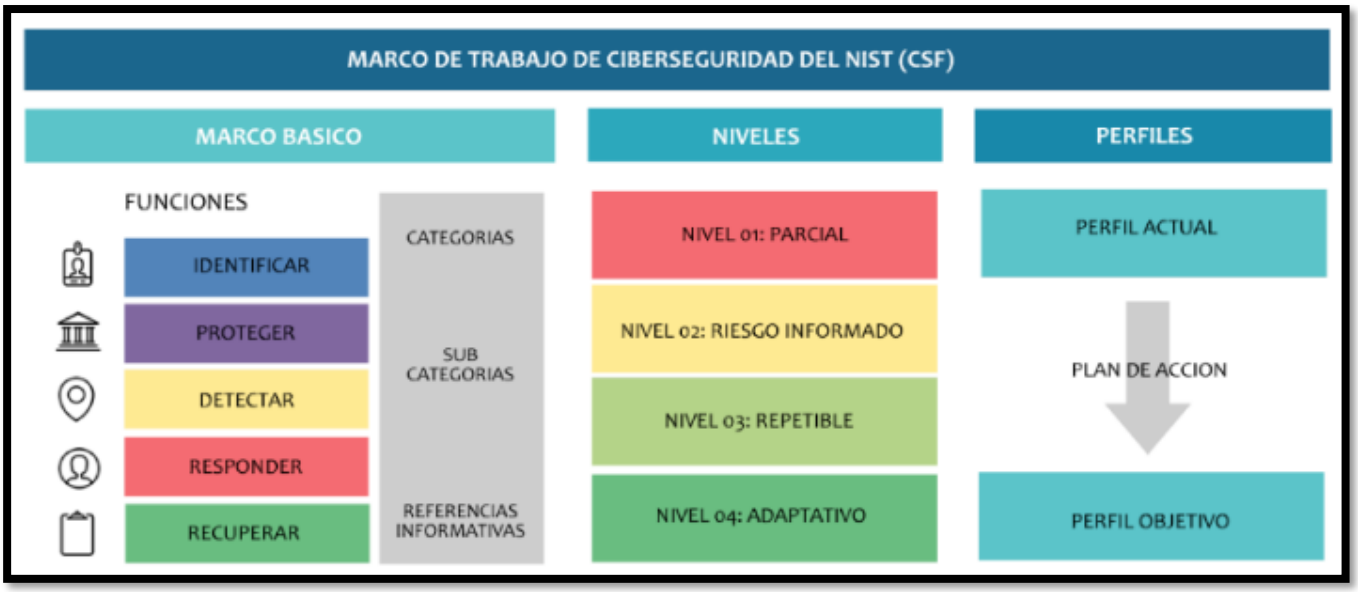
Aunado a esas funciones que son principales dentro del marco, se utilizan 3 elementos de orden: categorías, subcategorías y referencias informativas; los cuales tienen como objetivo identificar qué herramientas se utilizarán y cómo se aplicarán al gestionar los riesgos asociados a la seguridad de la información.

Ahora bien, el segundo componente del marco de referencia corresponde a “los niveles de implementación” mismos que proporcionan un contexto sobre cómo la organización percibe y administra el riesgo de seguridad cibernética; por tanto, esos niveles (parcial, riesgo informado, repetible y adaptables) apoyan la toma de decisiones en relación con las dimensiones de los procesos y su relación con la priorización, criticidad y características de los recursos involucrados.

Seguidamente, el componente denominado: “Perfiles del marco” es la alineación de las funciones, categorías y subcategorías con los requisitos organizacionales, la tolerancia al riesgo, los recursos, entre otros factores que brindan un escenario holístico para lograr establecer una hoja de ruta orientada a reducir el riesgo de seguridad cibernética.

Con el objetivo de representar visualmente la arquitectura antedicha de manera completa, en la siguiente imagen se puede apreciar los términos referenciados en su respectivo orden:

Imagen N°3
Arquitectura del marco de trabajo de ciberseguridad del NIST



Fuente: Marco Ciberseguridad del NIST

En resumen, la utilización de este marco de referencia entre otras cosas es capaz de brindar un diagnóstico actualizado del entorno tecnológico, los factores que afectan positiva o negativamente, la identificación del objetivo deseado en relación con los temas vinculados a seguridad cibernética e indudablemente una herramienta para apoyar la toma de decisiones.

Finalmente, y con el fin de brindar más insumos asociados al asunto tratado en esta misiva, en el Anexo 1 “Ciberseguridad Marco NIST”, se adjunta un documento emitido por la Organización de Estados Americanos (OEA), en el cual compila detalles relevantes del marco de referencia, en cuanto a su historia, composición; versiones y mecanismos de evolución; cómo utilizarlo; e inclusive ejemplifica casos de uso.

2.3. Sobre la educación en materia de ciberseguridad

Los estudios y pronósticos publicados en medios de información aseveran que existe una brecha entre los ciberdelincuentes y especialistas en seguridad. En este caso, el mensaje es reincidente para alertar sobre la escasez en educación tanto para los usuarios de la tecnología (aspectos básicos de ciberseguridad) y los profesionales a cargo de la infraestructura TIC (diferentes niveles de conocimiento y especialización).

Lo anterior, según lo confírmala página web “elEconomista.es” en su publicación del 28 de abril del 2022, titulado “La brecha de competencias en ciberseguridad provocó el 80% de los problemas de seguridad”, citando:

> *"Fortinet®, líder global en soluciones de ciberseguridad integradas y automatizadas, ha desvelado en su Informe sobre la brecha de habilidades en Ciberseguridad 2022 que la escasez de competencias en ciberseguridad conlleva múltiples retos y repercusiones para las organizaciones, como la aparición de brechas de seguridad y las consiguientes pérdidas económicas. En consecuencia, la falta de habilidades sigue siendo una de las principales preocupaciones de la alta dirección y se está convirtiendo cada vez más en una prioridad de la junta directiva. El informe también sugiere formas de abordar la brecha de competencias, como la formación y las certificaciones para aumentar la educación de los empleados.*
>
> *Para Sandra Wheatley, SVP de Marketing, y comunicación de inteligencia de amenazas e influencer en Fortinet, "nuestro informe constata que la brecha de competencias no es sólo un reto de escasez de talento, sino que también está afectando gravemente a los negocios, convirtiéndose en una de las principales preocupaciones de los empresarios de todo el mundo (…) "*

Es decir, las organizaciones han llegado a niveles sin precedentes en relación con la digitalización de procesos y eso ha conllevado a la exposición a riesgos tecnológicos, prueba de ello es el aumento exponencial del número de ciberataques y delitos digitales.

Ante esa situación, la educación es la mejor arma contra los ciberdelitos y la CCSS podría gestionar actividades de concientización, entrenamiento y capacitación para los consumidores y encargados de servicios TIC, considerando al menos los siguientes elementos:

- Implemente políticas para la ciberseguridad, considerando entre ellas la educación.
- Planificar la formación de expertos en ciberseguridad.
- Complementar la inducción a funcionarios sobre el uso y aprovechamiento de las TIC con entrenamientos sobre seguridad informática y de la información.
- Concientizar de manera continua a los consumidores de servicios TIC sobre temas asociados con la protección de activos de información.
- Enseñar sobre las amenazas cibernéticas y la responsabilidad.
- En contrataciones externas valorar la solicitud de recurso humano debidamente certificado en materia de ciberseguridad.
- Capacite y sea insistente sobre la necesidad de establecer contraseñas seguras, manejar datos sensibles y utilizar de manera adecuada los medios de comunicación.

En resumen, la educación referente a la ciberseguridad, sin duda es un tema de vital importancia para la Institución ya que tiene la posibilidad de brindar sostenibilidad a la transformación digital y mitigar en lo correspondiente a la exposición a riesgos tecnológicos.

3. CONSIDERACIONES FINALES

Dado el ambiente de innovación y transformación digital en el que se encuentra inmersa la Institución, así como del aumento de ciber incidentes complejos y sofisticados, resulta necesario prever los ataques informáticos e invertir recursos para gestionar los riesgos TIC, por medio de una estrategia o modelo de ciberseguridad con el detalle de elementos cruciales de cara al futuro.

Si bien es cierto, la institución conoce cuál es ese modelo meta para establecer un Gobierno de TIC y Seguridad de la Información aún no se ha implementado en la CCSS, pese a que la propuesta fue emitida por la firma PwC en el 2017.

Ante ello, la gestión de riesgos debe de ser objeto de análisis de los diferente involucrados a nivel estratégico, táctico y operativo, para generar acciones urgentes y prioritarias a fines con la prevención y mitigación de actos que puedan afectar: la reputación de la Institución; realización de labores en materia de salud, pensiones y recaudación patronal; la confidencialidad, integridad y disponibilidad de la información.

En línea con lo anterior, y conociendo el estado de la iniciativa de gobernanza de la seguridad, se podrían valorar por esa Administración: ejecutar medidas integrales en materia de ciberseguridad que se encuentren en armonía con el modelo meta; gestionar acciones urgentes y prioritarias en atención al contexto actual donde se han presentado eventos a nivel mundial y nacional en torno a los ciberataques.

En ese sentido, debemos recordar que la CCSS se enfrenta a grupos seriamente organizados financiados inclusive por gobiernos, que utilizan tecnología de alta gama para llevar a cabo sus planes delictivos. Por ello, al priorizar la puesta en marcha de las iniciativas asociadas a ciberseguridad, se estaría entregando a la Institución la seguridad razonable respecto de la protección de la información, reduciendo riesgos y vulnerabilidades, en el corto plazo; en apego a lo indicado en las *Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones*, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "Seguridad y Ciberseguridad", citadas estas al inicio de este documento.

En virtud de lo expuesto, se previene y advierte a esa Administración, con el propósito de que se adopten las medidas pertinentes, en la mitigación de vulnerabilidades; la entrega de resultados en tiempo y forma; y la adopción de mejores prácticas sometidas a valoración y revisión según corresponda tales como las esbozadas en esta misiva.

Finalmente, es relevante manifestar que esta Auditoría se encuentra en la mayor disposición de apoyar la gestión que desarrolle esa Administración ante la temática expuesta, conforme nuestras potestades y competencias.

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

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.05.03 16:03:42 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RAHM/OMG/lbc

Anexos:

1- Anexo 1 "-Ciberseguridad Marco NIST", emitido por la Organización de Estados Americanos (OEA).

C. Doctor Randal Álvarez Juárez, gerente, Gerencia Médica-1100
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 Tecnología-1107
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia de Pensiones-9108
Licenciada Xinia Fernández Delgado, directora, Dirección de Comunicación Organizacional -1115
Licenciado Walter Campos Paniagua, director, Direccion Administración y Gestión de Personal-1131
Auditoría

Referencia: ID-74860