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

AS-AATIC-108-2022
22 de junio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

Doctor
Randall Alvarez 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 TECNOLOGÍA - 1107

Licenciado
Jaime Barrantes Espinoza, gerente,
GERENCIA DE PENSIONES - 9108

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

Estimados señores:

ASUNTO:	**Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico.**

Esta Auditoría 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 consecuente al 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, emite la siguiente asesoría sobre aspectos relacionados con la estrategia de recuperación ante amenazas o desastres de origen tecnológico.

1. ANTECEDENTES

Como es ya conocido, la Caja Costarricense de Seguro Social (CCSS), recibió ciberataques que le obligaron a desactivar todos los sistemas informáticos de la Institución de manera preventiva.

Ahora bien, tras cumplirse más de 20 días de ese incidente, esta Auditoría tuvo conocimiento de las intenciones de restablecer el funcionamiento en determinados sistemas de información, tal y como se evidencia en algunas publicaciones de diarios nacionales.

En el Titular "CCSS estima que afectación por 'hackeo' dure al menos 2 meses" publicado por "CR Hoy.com" el 15 de junio del 2022, cita las estimaciones generales para la recuperación:

> *"La Caja Costarricense del Seguro Social (CCSS) advierte que la afectación por el hackeo a sus sistemas se mantenga por al menos 2 meses.*
>
> *Así lo dio a conocer este miércoles en conferencia de prensa, Álvaro Ramos, presidente ejecutivo de la institución.*
>
> *"Yo prefiero dar la mala noticia y si después es menos enhorabuena, pero mejor preparémonos como sociedad a que estos ciberpiratas nos hicieron un daño inmenso a esta importantísima institución sin los sistemas que necesita por al menos 2 meses", advirtió el ejecutivo.*
>
> *Ramos puso como ejemplo nuevamente el escenario que enfrentó Irlanda, donde el daño por cibernético afectó por 3 meses.*
>
> *Al corte de este 15 de junio, la institución dio a conocer que los ciberdelincuentes vulneraron un 81% de los servidores.*
>
> *Ramos manifestó que aún queda un 2% de los equipos por revisar."*

Según la publicación del 16 de junio del 2022, realizada por diario "La Nación" titulada "CCSS reactivará plataforma SICERE para recaudación en línea", menciona el restablecimiento de un conjunto de aplicativos, a saber:

> *"La Caja Costarricense de Seguro Social (CCSS) informó este jueves de que reactivará su plataforma en línea del Sistema Centralizado de Recaudación (Sicere), lo que permitirá a los patronos realizar los cambios correspondientes a la planilla del mes de mayo 2022, por medio de la Oficina Virtual de la entidad.*
>
> *La habilitación se iniciará a partir del martes 21 de junio y desde ese día hasta el viernes 24 los patronos podrán hacer la presentación de la planilla.*
>
> *Asimismo, en el caso de los empleadores denominados "grandes clientes", que presentan su planilla por medios magnéticos (archivos.txt), se estarán recibiendo los cambios por los medios habituales, a partir del lunes 20 y hasta el jueves 23 de junio.*
>
> *El gerente financiero de la CCSS, Gustavo Picado Chacón, expresó que "se ha hecho un gran esfuerzo por parte de los equipos técnicos del Sistema Centralizado de Recaudación (Sicere), en coordinación con la Dirección de Tecnologías de Información y Comunicaciones, para reactivar el Sicere en sus principales servicios de cara a los patronos y trabajadores del país, logrando restablecer a casi 20 días del ataque los servicios relacionados con este importante sistema".*
>
> *Con respecto al pago de las planillas patronales, se han dispuesto como fechas de pago para aquellas del mes de mayo, el martes 28, miércoles 29 y jueves 30 de junio, días que se consignarán en las facturas, una vez hechas estas para las planillas, por parte del patrono. Dichos abonos se podrán realizar mediante los mecanismos habituales de Sicere.*

La CCSS detalló que, a partir del martes 21 de junio, en la Oficina Virtual CCSS se habilitarán otros servicios para trabajadores y patronos, que habitualmente se encuentran disponibles en este servicio web, como las consultas de órdenes patronales digitales, reportes de salarios, estudios de cuotas, actualización de cuentas IBAN para pago de incapacidades, entre otros."

2. OBSERVACIONES

Si bien es cierto, este Ente Fiscalizador ha emitido recientemente los productos AS-AATIC-072-2022 del 10 de junio del 2022, sobre la gestión de crisis y AS-AATIC-088-2022 del 16 de junio del 2022, referente a la continuidad del negocio, los cuales incluyen reseñas al asunto mencionado en esta misiva; es menester de esta Auditoría especificar las siguientes observaciones que esa Administración podría considerar al desarrollar o perfeccionar una estrategia exitosa de recuperación.

2.1 Inventario de los activos TIC[1]

El plan de recuperación ante desastres siempre debe comenzar con un inventario de todos los activos de TI[2], a nivel de equipamiento y software, este paso es necesario para visualizar la complejidad del entorno y evitar omitir algún detalle en el restablecimiento de los servicios.

Lo anterior, en alineamiento a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, en el apartado "Administración Infraestructura Tecnológica", en el cual refiere:

"La institución debe implementar prácticas formales que permitan mantener identificados y actualizados los activos de TI, mediante inventarios de recursos tecnológicos instalados en la organización (hardware, software, aplicaciones, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas."

En consecuencia, considerando todos los activos, incluidos los servidores, terminales de almacenamiento, aplicaciones, datos, equipamiento de red, puntos de acceso y dispositivos de red que deben ser valorados y certificados en relación con su escaneo e inmunización (según corresponda); en aras de tener certeza sobre la mitigación de los riesgos asociados con las amenazas identificadas por los equipos técnicos de la CCSS en materia de ciberseguridad u otras vulnerabilidades a las que pueda estar expuesta la Institución.

En ese sentido, visibilizar la ubicación física de cada activo, condición lógica, interconexión a la red y de más aspectos, generará un insumo valioso para identificar los elementos primordiales de la plataforma tecnológica, nivel de dependencia de los usuarios, así como otras variables propias de los activos que son utilizadas para la toma de decisiones.

2.2 Evaluación y priorización de riesgos

Seguido al mapeo de todos los activos de TIC, el identificar las posibles amenazas internas y externas (actuales y venideras) es necesario dentro de un plan de recuperación, en aras de estimar de manera progresiva, cuáles serían los escenarios y el accionar de la Administración.

En ese sentido, los expertos recomiendan incorporar o verificar los niveles de probabilidad de que ocurran las amenazas, estimar su impacto desde el ámbito de negocio y/o tecnológico; esto con el objetivo de priorizar las actividades a seguir según los planes de continuidad y contingencia.

[1] Las Tecnologías de la Información y las Comunicaciones (TIC).
[2] La tecnología de la información (TI)

Además, examinando la oportunidad que tienen los mecanismos en materia de ciberseguridad, ya implementados en la Institución, en función de mitigar los riesgos tecnológicos detectados. Lo anterior, considerando el contexto actual de la CCSS y determinando si existen recomendaciones básicas por atender o requieren de una labor prioritaria en su ejecución, tales como:

- Implementación de doble factor de autenticación en sistemas y redes sociales.
- Utilización de contraseñas seguras y automatización de proceso de monitoreo (cambios periódicos, usuarios inactivos, cambios de puestos, detección de patrones de comportamiento, entre otras variables)
- Garantía de sistemas operativos y de información actualizados.
- Monitoreo constante de programas sin autorización o pirateados.
- Automatización en la detección de amenazas.
- Aseguramiento de conexiones a la red institucional, evitando enlaces a través de redes públicas o inseguras
- Gestionar la adecuada configuración de dispositivos, evitando puertos o enlaces que funcionen como "entradas traseras".
- Premisa de mantener al menos un respaldo fuera del sitio (de ser posible en la nube)
- Disponer de del plan de recuperación de desastres y de continuidad de negocio efectivo.
- Labor entorno a campañas de educación a los usuarios sobre los riesgos de ciberseguridad, manejo de correo, detección de alertas en los equipos finales, tipos de vulnerabilidades, entre otros elementos.

Lo anterior, en alineamiento a lo señalado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, descrito en el apartado la "Gestión del Riesgos Tecnológicos":

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

En otras palabras, como parte del restablecimiento de servicios TI, se debe valorar las condiciones digitales de la Institución, no solo para sobrevivir o reanudar a la normalidad, sino para adaptarse al nuevo entorno. Así las cosas, es necesario mantenerse alerta a las nuevas amenazas, formas de cibercrimen, recomendaciones de mejora, requerimientos en materia de disponibilidad de la plataforma tecnológica y la innovación digital ofrecida nivel de mercado.

2.3 Criticidad de las aplicaciones y los datos

Aunado a lo anterior, es de vital importancia clasificar los datos y aplicaciones de acuerdo con el impacto que puede percibir la Institución ante un inadecuado tratamiento de la información o la desconexión prolongada de los sistemas informáticos.

Lo anterior, en alineamiento a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, en el apartado la "Arquitectura empresarial", a saber:

> *"La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información.*

(…) La institución debe disponer de un modelo de clasificación de datos e información, según criterios y requisitos legales, de valor, según el nivel de criticidad y susceptibilidad a divulgación o modificación no autorizada. La Unidad de TI se basará en este modelo para establecer las directrices de seguridad y protección de los datos e información institucionales."

En ese sentido, evitando generalizar la situación, porque la estrategia de recuperación ante ciberataques puede ser diferente para cada aplicación o conjunto de datos. Por ello, agrupar o segmentar los activos con características similares permitirá implementar un plan acorde a las diferentes necesidades institucionales.

2.4. Definición de los objetivos de recuperación

Es relevante mencionar que los activos y datos tendrán diferentes objetivos de recuperación. Por ejemplo, un repositorio crítico o archivo con informaciones históricas de una actividad, puede tener objetivos de restablecimiento agresivos, esto porque la organización no debe perder ninguna transacción o crear lapsos sin registros digitales.

Por otro lado, un sistema interno heredado puede tener objetivos de recuperación menos estrictos porque los datos involucrados no cambian con mucha frecuencia, o existen otros mecanismos efectivos para respaldar la información.

En otras palabras, la definición de objetivos de recuperación se puede observar al tomar la decisión de recuperar información o asumir su pérdida. En ese sentido, la construcción de una estrategia que determine ese accionar debe valorar la criticidad de las aplicaciones; relevancia y sensibilidad de los datos; inversión y/o esfuerzo de labores por desarrollar; entre otros aspectos.

Por todo lo anterior, adquiere relevancia la premisa de mantenerse vigilantes al cumplimiento de la norma que refiera a esos casos específicos, entre ellas el Reglamento a la Ley de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales, particularmente al señalarse en el Capítulo IV, lo siguiente:

"Artículo 34. De las medidas de seguridad en el tratamiento de datos personales. El responsable, deberá establecer y mantener las medidas de seguridad administrativas, físicas y lógicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Reglamento. Se entenderá por medidas de seguridad el control o grupo de controles para proteger los datos personales.

Artículo 38. Vulnerabilidad de seguridad. El responsable deberá informar al titular sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá cinco días hábiles a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

Dentro de este mismo plazo deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan."

2.5. Determinación de herramientas y técnicas adecuadas

Existen numerosas soluciones que apoyan la temática recuperación ante ciberataques desde el ámbito estratégico, táctico y operativo, las cuales deberían ser valoradas por las instancias correspondientes.

En ese sentido, esas herramientas y técnicas pueden apoyar la misión de: proteger a la organización, crear un perímetro de seguridad avanzado, administrar la gestión de riesgos, coadyuvar al desempeño de roles y responsabilidades, crear vanguardia tecnológica, entre otras actividades.

A continuación, se citan algunas soluciones reconocidas, a saber:

- Plan de continuidad del negocio (Business Continuity Plan o BCP).
- Norma ISO 22301, basada en un compilado de prácticas orientadas a gestionar la continuidad de un negocio.
- Arquitecturas de recuperación y respaldo basados en sistemas de espejo, replicación sincrónica, computación en la nube, virtualización, sitio alterno y otras tecnologías para la alta disponibilidad de datos.
- Implementación de soluciones bajo enfoques de seguridad, adaptativos y predictivos que permita prevenir, detectar y dar respuesta a incidentes.
- Herramientas de monitoreo y actualizaciones asociadas con el uso óptimo de los recursos tecnológicos, bajo la premisa de entregar continuidad y sostenibilidad en las operaciones institucionales.
- RPA (Robotic Process Automation) para la contribución de acelerar procesos críticos, y proporcionar tranquilidad al garantizar la continuidad del negocio en determinados momentos.

Todo lo anterior, siendo consecuentes a la necesidad de investigar sobre las soluciones que puedan resultar de utilidad para la CCSS, tal y como lo propone las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021; detallado en el proceso “Gestión de TI”:

> *“La institución debe implementar y mantener prácticas de gestión de las TI, que defina formalmente los siguientes componentes para la entrega de servicios al nivel de tecnologías de información en alineación con el marco estratégico y el modelo de arquitectura empresarial:*
>
> *(…) Investigación sobre tecnologías emergentes que permitan a través de su eventual incorporación, la innovación y mejora continua al nivel institucional para el logro de los objetivos y la entrega de valor público.”*

En otras palabras, ese accionar significaría una alternativa que puede generar más confianza a la Institución, en particular al brindar servicios cuya disponibilidad es inmediata, tanto a nivel de procesos médicos, como financieros. Lo anterior, ante el riesgo de paralización del servicio, pérdidas (atención al usuario, económicas y de datos), así como del cumplimiento de indicadores de tiempos por objetivos de recuperación (RTO) y puntos por objetivos de recuperación (RPO).

2.6 Participación de entidades o empresas expertas en TI

Ante la necesidad particular de la organización, el ente rector en TI puede consultar a entidades de gobierno, socios estratégicos y proveedores para asegurarse de que la institución está aprovechando al máximo la solución o servicios disponibles, y a partir esos contactos obtener acceso a software, capacitación a nivel de usuarios, formación de profesionales, consultorías, entre otros aportes valiosos en el contexto actual y sin implicar costos adicionales.

Lo anterior, considerando lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021; en su apartado “Gobernanza TI”, a saber:

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

Una vez se consulte a las partes interesadas y de ser necesario, se podría valorar la necesidad de una empresa experta en TI para que apoye la atención de requerimientos debidamente justificados y acorde a las normas para la contratación y adquisición de bienes y servicios tecnológicos.

2.7 Documentar y comunicar la estrategia de recuperación

En un escenario de desastre, se necesita una estrategia documentada; en ese sentido, la tarea consiste en detallar las consideraciones antes, durante y después de la emergencia, así los funcionarios que lo usarán conocerán el panorama completo para trabajar en la recuperación correspondiente.

De esa manera, integrando esfuerzos en una misma dirección y evitando dejar a la organización vulnerable si un funcionario especifico no está disponible durante un incidente o se genera una acción individualizada.

A ese respecto, las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, en el apartado la "Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos", cita sobre la necesidad de comprensión de la estrategia a seguir:

> *"La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas (...)"*

2.8 Actualizar y evaluar el plan de recuperación

Una vez documentada la estrategia y cumpliendo la definición de variables respectivas, se podrá disponer de un plan de recuperación ante desastres, el cual debe considerarse como un instrumento dinámico.

A ese respecto, es significativo revisarlo con regularidad, tomando las previsiones particulares, por ejemplo, que el personal clave puede estar en un periodo "fuera de oficina" o cambiar su empleo; incorporación o baja de sistemas operativos o software de procesos; cambios de proveedores; entre otros aspectos por contemplar en el plan de recuperación.

Es decir, el propósito del documento es proyectar el estado actual de la institución, por ello la necesidad de actualizarle de manera constante; a su vez evaluarlo entorno con las exigencias organizacionales.

Aunado a lo anterior, deben existir pruebas o ejercicios para determinar la disponibilidad y efectividad de los mecanismos de contingencia en materia TI, bajo el deber de asegurar el propósito de las soluciones durante el traslado de la operación, el trabajo en continuidad y luego el retorno al sitio principal, esto en el menor tiempo posible.

En ese sentido, 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, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, en el apartado "Aseguramiento", en el cual refiere:

> *"La Unidad de TI debe incorporar prácticas de valoración para el aseguramiento sobre la entrega de servicios y el uso óptimo de los recursos tecnológicos instalados para apoyar a la institución en la continuidad de sus operaciones, salvaguarda y protección de la información y activos asociados y la implementación de iniciativas para el logro de los objetivos institucionales."*

3. CONSIDERACIONES FINALES

La Caja Costarricense del Seguro Social (CCSS), dentro de su gestión y servicios que presta a la ciudadanía depende de la información, sistemas y soluciones tecnológicas, ante ello surge la necesidad de establecer una estrategia acorde a las obligaciones institucionales.

Particularmente, refiriéndonos a la estrategia de recuperación ante el ciberataque sufrido el 31 de mayo del 2022 y que afecta los procesos de salud, pensiones y recaudación patronal.

En ese sentido, se pretende que a partir de las observaciones inmersas en esta misiva, se valore la definición de la estrategia más apropiada a los requerimientos específicos de la Caja, su apetito al riesgo y de la disponibilidad de recursos.

Además, recordando que esa Administración podrá aplicar las mejores prácticas relacionadas con ciberseguridad y continuidad del negocio; tanto en la definición de estrategias, como en la toma de decisiones sobre las herramientas y/o soluciones a implementar.

A ese respecto, involucrando a los sistemas de información, aplicativos, datos, equipamientos tecnológicos y otros elementos vitales en cualquier plan de continuidad del negocio, así como los contingenciales de los servicios de apoyo, entre ellos los correspondientes a las TIC.

Así mismo, destacando la necesidad inminente de fortalecer las soluciones de alta disponibilidad y la generación de acciones preventivas que prevengan y minimicen la posibilidad de ocurrencia ante desastres a nivel nacional.

Todo lo anterior, con el objetivo de ser resilientes y generar confianza en los servicios que obtienen apoyo por parte de las TIC, manteniendo la continuidad de las operaciones, pese al costo en inversión necesaria para prever este tipo de eventos (mínimo, en comparación a una nueva materialización del riesgo), de ahí la relevancia de la temática de valoración y priorización detallada en este oficio.

De esa manera, marcando la diferencia para futuros incidentes en cuanto no perjudicar las actividades sustantivas, disminuir el daño de la imagen institucional o en caso de materializarse el riesgo, prever de forma anticipada una solución conforme a las necesidades de los procesos.

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio, con el objetivo de incentivar la capacidad de la Institución para recuperar y restablecer el componente TI después de la interrupción en sus sistemas de información que aún afecta a la CCSS; y el cual es un aspecto tecnológico que incumbe a la continuidad del negocio.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.22 16:33:59 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/ghc

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