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

AS-AATIC-093-2022
21 de junio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

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

Estimados señores:

ASUNTO:	**Oficio de asesoría referente a las previsiones relacionadas con los contratos de prestación de servicios por terceros eventualmente afectados por el ciberataque sufrido el 31 de mayo de 2022.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo de esta Auditoria, para el período 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre aspectos relacionados con la valoración de las posibles afectaciones en los contratos de prestación de servicios técnicos y profesionales contratados por la institución, a fin de que sean valorados para la toma de decisiones y acciones que compete a esa Administración, a raíz de los ataques cibernéticos sufridos por la institución el pasado 31 de mayo del 2022, lo que provocó la suspensión de los sistemas y servicios informáticos institucionales de manera preventiva.

En consonancia con lo anterior, esta Auditoría tiene conocimiento de la ejecución de los procedimientos de contratación promovidos entre los años 2016-2021, cuya finalidad es atender actividades relacionadas con el desarrollo de sistemas, soporte en la administración de eventos y seguridad de la información, filtrado de contenido dinámico y web, gestión del cambio y acompañamiento en las mejoras de los servicios, desarrollo e implementación del Modelo de Gobernanza y Gestión de TIC, licenciamiento de herramientas y certificados de seguridad, entre otros, lo que genera una erogación de alrededor ¢5,734,686,903.04 (cinco mil setecientos treinta y cuatro millones seiscientos ochenta o seis mil novecientos tres colones con 04/100) en conjunto, cuya ejecución podría verse afectada por la suspensión temporal de los servicios y sistemas de tecnologías de información y comunicaciones.

I. ANTECEDENTES

El 20 de abril del 2022, el portal de Recursos Humanos sufrió un ataque cibernético tal como lo informó el diario La Nación[1], en nota con el titular de “Portal de Recursos Humanos de CCSS sufre ataque cibernético”, indicando:

> *“Las plataformas digitales de las entidades públicas siguen siendo objeto de ataques cibernéticos. La Caja Costarricense de Seguro Social (CCSS) sufrió este miércoles una incidencia en su portal de Recursos Humanos, que obligó a activar una revisión integral de todos sus sistemas para determinar el alcance de lo ocurrido.*
>
> *El ingeniero Roberto Blanco Topping, director de Tecnologías de Información de la CCSS, detalló que una vez detectado el problema se procedió a blindar los accesos, dar de baja el portal y coordinar con los equipos técnicos para determinar si se produjo alguna extracción de información o de datos, o eventuales accesos a otras plataformas.*

[1] Diario La Nación 20 de abril de 2022

"Los equipos de monitoreo, humanos y en conjunto con las herramientas tecnológicas con las que se cuenta detectaron incongruencias con respecto a la gestión de datos en el portal de Recursos Humanos de la institución y se determinó que se había producido un ataque externo", detalló mediante un comunicado.

Posteriormente, el 31 de mayo de 2022, se registró en horas de la madrugada un nuevo ciberataque contra los servidores de la C.C.S.S., el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

En ese sentido, el Dr. Alvaro Ramos Robles, presidente ejecutivo de la institución el 1 de junio del 2022, en conferencia de prensa a medios nacionales, mencionó:

"La Manera en la que entraron los hackers dañó la forma en la que los usuarios pueden acceder a los sistemas y reparar estos accesos toma bastante más días de lo que se indicó inicialmente. Ya sí les podría adelantar que no se ve posible restaurarlos esta semana, preferiría no adelantar cuánto más, pero esta semana no va a hacer"

Aunado a lo anterior, el 6 de junio del 2022, se comunicó en el medio digital Crhoy, respecto al nivel de infección de institucional:

"La Caja Costarricense de Seguro Social ***confirmó que el 67 por ciento de sus servidores se infectaron tras los ciberataques*** *de la semana pasada.*

La Dirección de Tecnologías de Información y Comunicaciones (DTIC) de la Caja está concluyendo la revisión de 27.755 computadoras en todo el país, de las cuales 9.600 se identificaron como infectadas, lo que significa el ***27% del total de las terminales.***

De igual manera, se avanzó en la revisión de los 996 servidores de los cuales ***773 fueron revisados, encontrándose 665 infectados que representa el 67%,*** *informó la institución." (lo resaltado corresponde al original)*

Como resultado de lo anterior y como medida de contención del ataque, se procedió a la desconexión de los sistemas como el Expediente Digital Único en Salud (EDUS), Sistema Central de Recaudación (SICERE), Portal Web, Sistema de Farmacia (SIFA), entre otros, además del apagado de los equipos de usuario final conectados a la red institucional, con la finalidad de proceder al diagnóstico de las afectaciones.

Adicionalmente, mediante oficio GA-CAED-0260-2022 del 02 de junio del 2022, suscrito por el Dr. Mario Vílchez Madrigal, director a.i., del Centro de Atención de Emergencias y Desastres, comunicó al cuerpo gerencial, directores de sede, directores de red integrada de servicios de salud, directores regionales de sucursales, directores generales y administrativos financieros de hospitales y directores y administradores de área de salud, la declaratorio de estado de emergencia institucional por los ciberataques, en lo que interesa indicó:

"- Que existe una Declaratoria de Emergencia Nacional en todo el sector público debido a los ciberataques que han afectado la estructura de los Sistemas de Información, mediante Decreto No. 43542-MP-MICITT.

- Que la Caja Costarricense de Seguro Social, ha sido víctima de estos ciberataques, especialmente en la madrugada del día 31 de mayo del 2022.

- Que de acuerdo con los informes presentados por la Dirección de Tecnologías de Información y Comunicaciones al Centro Coordinador de Emergencias Institucional (CCEI) se tuvo que realizarla desactivación controlada de los servicios TI institucionales el 31 de mayo del 2022.

(…)

Procede a Validar el Estado de Emergencia Institucional, debido a los ciberataques sufridos por la Caja Costarricense de Seguro Social el 31 de mayo del 2022. De manera que, se solicita a todas las instancias aplicar las medidas necesarias para la atención de esta emergencia. Se instruye a mantener en operación los

Centros Coordinadores de Operaciones Central, Regionales y Locales y aplicar los mecanismos de excepción requeridos para la continuidad de los servicios. La Dirección de Presupuesto y el CAED informarán el procedimiento excepcional que se utilizará mientras los sistemas institucionales de TI sigan desconectados, mediante el cual se aplicará el Procedimiento para la gestión de la Reserva de Contingencia del Seguro de Salud (de la Caja Costarricense de Seguro Social).”

Finalmente, esta Auditoría ha tenido conocimiento de múltiples comunicados emitidos por la Dirección de Tecnologías de Información y Comunicaciones, relacionados con la atención de las afectaciones del ciberataque, en aspectos tales como; proceso de revisión de equipos de usuario local, procedimiento de revisión de servidores, procedimientos de limpieza de equipos, procedimientos de aplicación de Microclaudia, entre otros.

II. CONSIDERACIONES

En consonancia con lo anterior y dado que, como resultado del ciberataque sufrido el 31 de mayo de 2022, es previsible que la prestación de servicios contratados sea eventualmente afectada ante la imposibilidad de los proveedores de acceder a la red institucional, se debe garantizar que en los productos contratados se considere la aplicación de medidas, con la finalidad de identificar aquellos casos donde fue suspendido total o parcialmente su desarrollo y sus eventuales consecuencias en el proceso de pago de los mismos, así como en los tiempos de entrega.

Además, debería considerarse aquellos casos en los que se requiera una ampliación del bien contratado, con la finalidad de fortalecer las capacidades y el alcance de la respuesta al ciberataque o que se requieran para la puesta en marcha de los servicios, en cuyo caso su ampliación debe considerar la aplicación del marco normativo correspondiente.

Al respecto, el artículo 8 de la Ley General de Control Interno, respecto al sistema de control interno, establece:

“(…) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
b) Exigir confiabilidad y oportunidad de la información.
c) Garantizar eficiencia y eficacia de las operaciones.”

Así mismo, el Reglamento a la Ley General de Contratación Administrativa en su artículo 208 “Modificación Unilateral del Contrato”, establece:

“La Administración podrá modificar unilateralmente sus contratos tan pronto éstos se perfeccionen, aún antes de iniciar su ejecución y durante ésta, bajo las siguientes reglas:

a) Que la modificación, aumento o disminución del objeto, no le cambie su naturaleza, ni tampoco le impida cumplir con su funcionalidad o fin inicialmente propuesto.

(…)

d) Que se trate de causas imprevisibles al momento de iniciar el procedimiento, sea que la entidad no pudo conocerlas pese a haber adoptado las medidas técnicas y de planificación mínimas cuando definió el objeto.

El incremento o disminución en la remuneración se calculará en forma proporcional a las condiciones establecidas en el contrato original. En caso de disminución, el contratista tendrá derecho a que se le reconozcan los gastos en que haya incurrido para atender la ejecución total del contrato.”

Además, las Normas Técnicas para la Gestión y Control de las Tecnologías de Información promulgadas por el Ministerio de Ciencia, Innovación, Tecnologías y Telecomunicaciones, en su apartado X "Desarrollo, implementación y Mantenimiento de Sistemas de Información, establece:

> "*La unidad de TI debe aplicar prácticas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida.*
>
> *(…)*
>
> *La Unidad de TI debe aplicar las prácticas de aseguramiento del cumplimiento contractual y las prácticas de calidad asociadas para los casos en utilice soluciones desarrolladas y/o implementadas por proveedores externos."*

Ciertamente, la prestación de los servicios institucionales en la actualidad, responde en gran medida a la utilización de los sistemas y tecnologías de información que se han desarrollado, por lo que resulta de relevancia el adecuado control de los contratos en ejecución en la circunstancia actual de desconexión como medida de prevención ante el ciberataque recibido.

La circunstancia descrita eventualmente provocaría que los productos en desarrollo por parte de los proveedores sean afectados, alargando sus tiempos de entrega o en el cumplimiento de los cronogramas establecidos, dado que podrían carecer de los accesos necesarios a la plataforma TIC para lograr el objetivo planteado en cada caso. En esta condición excepcional, se debe considerar el establecimiento de mecanismos de control que permitan identificar las posibles afectaciones, así como las medidas a ejecutar para cada contrato.

Así mismo, en aquellos casos que se requiere la ampliación de objeto contratado, con la finalidad de asegurar una respuesta oportuna y adecuada a la situación planteada, se recuerda la consideración del marco normativo, con la finalidad de garantizar la legalidad de lo actuado.

Debido a lo anterior, y con el fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a esa Administración Activa, para que realice una valoración de los aspectos señalados, y eventualmente se fortalezca las medidas de control interno sobre este particular.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.21 14:54:22 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AAM/ghc

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