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

**AD-AATIC-078- 2022**
13 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
**GERENCIA GENERAL - 1100**

Máster
Idannia Mata Serrano, subgerente a.i
**DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1105**

Estimado (a) señor(a):

| | |
|---|---|
| **ASUNTO:** | **Oficio de Advertencia sobre la urgente necesidad de disponer de un sitio alterno de procesamiento de datos, dada la afectación sufrida en la prestación de servicios por el ciberataque del 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 necesidad de contar con un sitio alterno de procesamiento de datos 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 acciones ejecutadas por la Administración a efectos de dotar a la institución con un sitio alterno de procesamiento de datos que eventualmente permitiría la continuidad de los servicios y disminuiría el impacto ante la interrupción materializada por el ataque mencionado u otros riesgos ya identificados, mediante una alternativa que, de acuerdo a su alcance, permitiría el funcionamiento continuo de los servicios tecnológicos, sin afectación para el usuario final.

Sin embargo, se evidenció que en la actualidad aún se carece de ese sitio alterno. En el presente documento, se verifica el estado actual de las gestiones llevadas a cabo por la Dirección de Tecnologías de Información y Comunicaciones, en esta materia.

## I. ANTECEDENTES

### I.I SOBRE EL CIBERATAQUE DEL 31 DE MAYO DE 2022

El 31 de mayo de 2022, se registró en horas de la madrugada un ciberataque a la C.C.S.S., que obligó en forma preventiva la desconexión de todos los servicios y sistemas informáticos, a fin de contener la afectación.

Dentro de los sistemas desconectados se encuentra 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 implementar las medidas correspondientes.

Adicionalmente, mediante oficio GA-CAED-0260-2022 del 02 de junio de 2022, suscrito por el Dr. Mario Vílchez Madrigal, director a.i., del Centro de Atención de Emergencias y Desastres, se comunicó la declaratoria de estado de emergencia institucional por los ciberataques:

*"- 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)."*

## I.II SOBRE EL CONCEPTO DE SITIO ALTERNO DE PROCESAMIENTO DE DATOS

Uno de los objetivos principales de la institución es garantizar la continuidad en la prestación de los servicios a los asegurados, dentro de este concepto es necesario recordar que se requiere de la implementación de diversos mecanismos entre los que se encuentran los planes de contingencia, de continuidad y de recuperación del negocio, entre otros.

En ese orden de ideas, con la finalidad de evitar la interrupción del negocio debe identificarse con claridad los riesgos a los que están expuestos los diversos procesos que se ejecutan, así como el nivel crítico de las herramientas, aplicaciones, sistemas y demás componentes de la infraestructura tecnológica, lo que permita establecer aquellos elementos que requieren de continuidad en su ejecución con la finalidad de no detener la marcha habitual de la institución.

Dentro de ese marco, el sitio principal de procesamiento de datos es el ambiente en el cual se alojan los recursos informáticos que soportan el negocio, el cual cuenta con los elementos necesarios para que la organización cumpla sus objetivos y se provean los medios tecnológicos necesarios para la operación cotidiana.

De forma tal que un sitio alterno es un ambiente de características similares al sitio principal donde se dará continuidad a las tareas consideradas de mayor importancia y criticidad para el negocio, en caso de materializarse un riesgo que implique la suspensión de los servicios.

Este sitio debe iniciar operaciones, de acuerdo con los protocolos incluidos en los planes de contingencia y continuidad, en el momento que se determine una afectación en el sitio principal. Por lo tanto, su efectividad depende de la compatibilidad de los elementos con el sitio principal en aspectos como software, apps corporativas, actualizaciones entre otros. Las capacidades que ofrezca el sitio alterno para la recuperación de las actividades incidirán directamente en su costo, el modelo en el cual se replican todas las funcionalidades y servicios del sitio principal representa una mayor inversión, en contrario al disminuir los elementos que soporta el monto es menor.

La importancia de disponer con este elemento dentro de la infraestructura tecnológica institucional está determinada por la posibilidad de continuar prestando los servicios ante eventuales interrupciones por la materialización de riesgos de origen humano (huelgas, sabotajes, ciberataques, incendios), naturales (inundaciones, rayos, terremotos) o tecnológicos (carencia de fluido eléctrico, daño en servidores, afectación de telecomunicaciones); aportando un elemento que permita responder a estas eventualidades en el menor tiempo de respuesta, a efectos de disminuir la afectación a los usuarios internos y externos en aspectos tales como atención en salud, pensiones, pago a proveedores, pago de incapacidades, control de inversiones; así como en los posibles daños que sufra la imagen de la CCSS ante la imposibilidad de retomar con algún grado de normalidad sus funciones.

## I.III SOBRE LAS ACCIONES EJECUTADAS CON LA FINALIDAD DE IMPLEMENTAR EL SITIO ALTERNO DE PROCESAMIENTO DE DATOS.

En relación con esta materia, el 13 de noviembre de 2014, en sesión N°8751, la Junta Directiva de la Caja Costarricense de Seguro Social, en el artículo 10° indicó lo siguiente:

> *"ARTICULO 10°*
>
> *Asimismo, y acogida la propuesta del director Alvarado Rivera, se solicita a la Gerencia de Infraestructura y Tecnologías que tome todas las medidas que corresponda para atender lo relativo al citado proceso de intervención y, en el caso particular del de la plataforma tecnológica central y el sitio alterno, que se presente una propuesta de solución."*

En atención a dicho acuerdo, el 19 de marzo de 2015 se realizó la presentación ante la Junta Directiva de la propuesta de solución concebida por la Dirección de Tecnologías de Información y Comunicaciones, para dar atención a la necesidad institucional de disponer de un Centro de Datos Principal y un Centro de Datos Alterno.

De conformidad con lo anterior, el Jerarca Institucional acordó en el artículo 18° de la sesión N°8768[1], dar por recibido el informe de avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional, así como solicitar que en un plazo de tres meses se presente el siguiente informe.

En ese mismo orden de ideas, el Proyecto fue presentado en la sesión N°8831[2] como parte de las Líneas Estratégicas en Tecnologías de Información y Comunicaciones, donde se dio por conocida la propuesta de trabajo a desarrollar en estos aspectos, siendo que se continúe con la presentación de avances alcanzados.

Mediante oficio GG-DTIC-636-2020 del 23 de octubre de 2020, el Máster Roberto Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones, remitió al Dr. Roberto Cervantes Barrantes, Gerente General, el documento "Informe de avance de del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), para Junta Directiva", en el cual incluyeron las acciones ejecutadas para el desarrollo tecnológico de la Caja Costarricense del Seguro Social, así las alternativas para la implementación del sitio alterno que se detallan seguidamente:

[1] Sesión de Junta Directiva del 19 de marzo del 2015
[2] Sesión de Junta Directiva del 10 de marzo del 2016

**Tabla No.1**
**Alternativas propuestas para el desarrollo del Centro de Procesamiento Principal y el Sitio Alterno**

| Alternativa | Descripción | Sitio Principal | Sitio Alterno |
|---|---|---|---|
| 1 | Centro de Datos como Servicio y CODISA. | Contratación de un Centro de Datos como Servicio (el suministro del equipamiento se incluye como parte del servicio). | CODISA como Sitio Alterno en las instalaciones actualmente rentadas por la CCSS (el equipamiento es adquirido por la CCSS). |
| 2 | Construcción de un Centro de Datos con equipamiento Leasing, y CODISA como Sito Alterno. | Construcción de un Centro de Datos propiedad de la CCSS. Operación de equipos por leasing a demanda. Contratación de servicios de administración, mantenimiento y operación. | • CODISA como Sitio Alterno en las instalaciones actualmente rentadas por la CCSS (el equipamiento es adquirido por la CCSS). |
| 3 | Centro de Datos como Servicio y Construcción de un Centro de Datos con equipamiento Leasing. | Contratación de un Centro de Datos como Servicio (el suministro del equipamiento se incluye como parte del servicio). | • Construcción de un Centro de Datos propiedad de la CCSS.<br>• Operación de equipos por leasing a demanda.<br>• Contratación de servicios de administración, mantenimiento y operación. |
| 4 | Centro de Datos como Servicio y Construcción. | Contratación de un Centro de Datos como Servicio (el suministro del equipamiento se incluye como parte del servicio). | • Construcción de un Centro de Datos propiedad de la CCSS.<br>• Adquisición de equipamiento tecnológico.<br>• Contratación de servicios de administración, mantenimiento y operación. |
| 5 | CODISA y Centro de Da-tos como Servicio del ICE. | Se mantienen las instalaciones actualmente rentadas por la CCSS en CODISA (el equipamiento es adquirido por la CCSS). | • Contratación de un Centro de Datos como Servicio (el suministro del equipamiento se incluye como parte del servicio). |
| 6 | CODISA, Nube y Centro de Datos Oficinas Centrales. | Se mantienen las instalaciones actualmente rentadas por la CCSS en CODISA (el equipamiento es adquirido por la CCSS). | • Incorporación de nubes públicas.<br>• Mejoras en la infraestructura del Centro de Comunicaciones en Oficinas Centrales. |

| | | | |
|---|---|---|---|
| 7 | CODISA, Nube y Centro de Datos ICE. | Se mantienen las instalaciones actualmente rentadas por la CCSS en CODISA (el equipamiento es adquirido por la CCSS) Incorporación de nubes públicas. | • Centro de Procesamiento Alterno por servicios con el ICE.<br>• Incorporación de nubes públicas. |
| **8** | **CODISA y Centro de Datos ICE.** | **Se mantienen las instalaciones actualmente rentadas por la CCSS en CODISA (el equipamiento es adquirido por la CCSS).** | **• Centro de Procesamiento Alterno por servicios con el ICE** |

**Fuente:** Informe de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional emitido por la Dirección de Tecnologías de Información y Comunicaciones, octubre, 2020. (lo resaltado no corresponde al original)

Aunado a lo anterior, el mencionado documento incluyó dictamen financiero sobre el costo de implementación y desarrollo de cada una de las alternativas propuestas, según se detalla a continuación:

**Tabla No.2**
**Resultados del Estudio de Mercado**
**alternativas propuestas para sitio alterno**

| Alternativa | Precio Menor | Precio Mayor |
|---|---|---|
| 1 | $37.308.768 | $63.342.144 |
| 2 | $49.561.671 | $78.364.463 |
| 3 | $86.870.439 | $141.706.607 |
| 4 | $47.657.600 | $74.612.479 |
| 5 | $38.316.478 | N/A |
| 6 | $12.522.032 | N/A |
| 7 | $23,320,067 | $33,397,652 |
| **8** | **$8,313,056.40** | **$16,888,265.12** |

**Fuente:** Informe de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional emitido por la Dirección de Tecnologías de Información y Comunicaciones, octubre, 2020. (lo resaltado no corresponde al original)

Posteriormente, en el artículo 132° de la sesión 9189 de Junta Directiva celebrada el 24 de junio de 2021, se acordó:

***"ARTICULO 132º***

*Se conoce oficio N° GG-DTIC-2432-2021, de fecha 6 de mayo de 2021, suscrito por el Ing. Roberto Blanco Topping, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones mediante el cual presenta el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (centro de datos)*

*Solicitud para que la Junta Directiva brinde aval a la estrategia propuesta para implementar la Alternativa #8 del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos Principal y Centro de Datos Alterno) y se apruebe para que la Dirección de Tecnologías de Información y Comunicaciones inicie el proceso de contratación directa con Instituto Costarricense de Electricidad mediante la excepción entre entes de derecho público. (…)*

***ACUERDO SEGUNDO:***

*Aprobar la estrategia propuesta para implementar la Alternativa #8 del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos Principal y Centro de Datos Alterno).*

***ACUERDO TERCERO:***

*Se Instruye a la Dirección de Tecnologías de Información y Comunicaciones para que inicie el proceso de contratación directa con el Instituto Costarricense de Electricidad mediante la excepción entre entes de derecho público."*

Mediante oficio GG-DTIC-7431-2021, del 14 de diciembre de 2021, suscrito por el Ing. Roberto Blanco Topping, subgerente a.i de la Dirección de Tecnologías de Información y Comunicaciones, solicitó al Dr. Roberto Cervantes Barrantes instrucción respecto a la adquisición del servicio administrado para el fortalecimiento de la infraestructura redundante del centro de procesamiento primario y el centro de procesamiento alterno, en lo que interesa indicó:

*"La subdirección de la Dirección de Tecnologías de Información y Comunicaciones inició el proceso previo de contratación directa, emitiendo los requisitos de la compra mediante oficio GG-DTIC-6959-2021 del 10 de noviembre de 2021, a la Subárea de Gestión Administrativa, para recibir la oferta formal por parte del ICE.*

*Sin embargo, esta Jefatura mediante oficio GG-DTIC-6944-2021 del 22 de noviembre de 2021 rindió un informe a Gerencia General, en donde se expuso la preocupación que en todos los estudios previos, se hayan utilizado términos de referencia con características técnicas que solo podían cumplir empresas que representan a la marca CISCO, lo anterior conocedores que según el oficio AI-1001-2020 del 05 de agosto de 2020 suscrito por el Auditor Interno, se cuestionara sobre este mismo tema, ya que se concluyó que eso limita la participación de potenciales proveedores en virtud del requerimiento de integración y compatibilidad del 100 por ciento a las plataformas y dispositivos CISCO, igualmente cuestionado por equipos técnicos que conformó la Gerencia General para la revisión de ese oficio de auditoría. Sobre este oficio no hemos recibido respuesta.*

*De conformidad con lo anterior, solicitamos el criterio a esa Gerencia de cómo proceder en la contratación que se encuentra suspendida, por cuanto a la fecha no se cuenta con la certeza del resultado del proceso de investigación, por lo que esta Dirección considera los siguientes escenarios:*

1- *Continuar con el proceso de contratación con los criterios previos que sustentaron el Acuerdo de Junta Directiva artículo 132° de la sesión N° 9189, celebrada el 24 de junio del año 2021.*

2- *Quedar a la espera del resultado de la investigación ordenada por Gerencia General.*

3- *Iniciar un proceso de contratación nuevo valorando la administración características técnicas apegadas a la necesidad institucional y asegurando los principios de contratación administrativa desde el estudio de mercado, o*

4- *Cualquier otra opción que considere la Gerencia General."*

En respuesta a lo anterior, el Dr. Roberto Cervantes Barrantes, Gerente General, mediante oficio GG-0433-2022 del 24 de febrero de 2022, en lo que interesa señaló:

> *"Primero, debe tenerse claridad que la instrucción para la realización del procedimiento de contratación en cuestión fue dada directamente por la Junta Directiva para que fuera ejecutada por la Dirección de Tecnologías de Información y Comunicaciones (DTIC), como expresamente lo indicó el acuerdo tercero del artículo 132 de la sesión 9189 de 24 de junio de 2021 (…).*
>
> *En ese sentido, la decisión de contratar directamente con el ICE bajo la excepción de contratación entre entes de derecho público y de esta forma materializar la alternativa #8 del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional, fue tomada por la Junta Directiva, con base en la argumentación técnica expuesta en su momento por la propia DTIC mediante oficio GG-DTIC-2432-2021, en el cual, dicho sea de paso, se requería autorización para que esa Dirección desarrollara el correspondiente procedimiento de contratación con el ICE.*
>
> *Así las cosas, se tiene total claridad de que corresponde a la DTIC la realización del procedimiento de contratación administrativa, por ende, recae en la Dirección a su cargo el* ***deber de verificar la correcta realización del procedimiento*** *preseleccionado con estricto apego a la normativa que le resulta aplicable y los principios que instruyen a la contratación administrativa en general, lo que comporta que no sólo por el simple hecho de que la Junta Directiva haya instruido el uso de la excepción mencionada, esta se encuentra habilitada, sino que deben verificarse las condiciones y satisfacerse todos los requisitos exigidos por el ordenamiento jurídico para dicha excepción y así se debe dejar constancia en el correspondiente expediente electrónico de la contratación, al cual deberán adicionarse todos los estudios que fundamenten la adquisición en cuestión tanto a nivel técnico como a nivel de uso de la excepción para contratar entre entes de derecho público.*
>
> *Ahora bien, informa a este Despacho que al efectuar las actuaciones previas para la realización del procedimiento en cuestión, advierte que los "(…) estudios previos, se hayan utilizado términos de referencia con características técnicas que solo podían cumplir empresas que representan a la marca CISCO (…)", así las cosas, conociendo una serie de antecedentes institucionales como lo es el informe de auditoría interna AI-1001-2020 que cuestionó potenciales direccionamientos en compras para con dicha casa comercial, lo que podría estar sesgando la participación abierta de otros potenciales proveedores para las necesidades de redes en la CCSS; por lo que plantea cuatro escenarios y solicita se instruya cuál resulta más oportuno a los intereses institucionales (…).*
>
> *Ahora bien, dado lo explicado inicialmente en cuanto a que la Junta Directiva, en su condición de jerarca institucional instruyó directamente a la DTIC para la realización del procedimiento de contratación en cuestión, carece este Despacho de competencia para girar instrucción alguna que pueda contravenir lo dispuesto por el órgano colegiado, descartándose categóricamente que pueda utilizarse la opción expuesta en el escenario 4.*
>
> *Por su parte el escenario 1 (continuar con el procedimiento de contratación según lo instruido por Junta Directiva) no es algo que pueda instruir esta Gerencia General, sino que ya fue previamente dispuesto por Junta Directiva, por lo que efectivamente, salvo que se le exponga a Junta Directiva, razones técnicas que imposibiliten la continuación de la contratación, deberá acatar la instrucción recibida mediante el acuerdo tercero del artículo 132 de la sesión 9189.*

*En otras palabras, corresponde exclusivamente a la DTIC el liderazgo en desarrollo de la gestión desde su experiencia en el tema de tecnologías de información y comunicaciones careciendo este Despacho de competencia para generar una instrucción como la que ahora se pretende, ahora bien, se reitera que si por algún motivo se advierte una* ***imposibilidad de realizar la contratación*** *en los términos ordenados por la Junta Directiva, deberá hacerlo ver con los estudios correspondientes (financieros, técnicos, entre otros) y así exponérselo al colegiado quien fue el que instruyó la realización de contratación, para que este, con nueva fundamentación técnica pueda decidir sobre la eventual conveniencia de modificar lo inicialmente acordado sobre el tema.*

*Ahora bien, mantenerse a la espera (escenario 2) de los resultados que pueda arrojar las investigaciones que existen en relación con los hechos expuestos que podrían tener relación con la contratación de interés, tampoco puede entenderse como una opción válida, ya que no se dispone de un acuerdo posterior de Junta Directiva que haya suspendido o dejado sin efecto el acuerdo que instruyó a la DTIC la realización de la contratación de marras.*

*Por su parte la opción 3, iniciar un proceso de contratación valorando la administración características técnicas apegadas a la necesidad institucional y asegurando los principios de contratación administrativa, es una opción que entiende este Despacho debe estar integrada en la opción 1, de manera tal que al atender la instrucción de realizar el procedimiento de contratación con el ICE bajo la excepción de contratación entre entes de derecho público, este deberá efectuarse con estricto apego a la normativa y principios de contratación administrativa aplicables para dicha figura contractual.*

*Por último, se desprende del informe GG-DTIC-6944-2021, que el planteamiento o propuesta realizada por ICE que involucra a la marca CISCO, pudiera obedecer a insumos proveídos por la CCSS, cuando se señala:*
*"Sin embargo, revisando los antecedentes señalados en el oficio 9079-571-2021 del 12 de octubre de 2021, suscrito por el Sr. Walter Redondo Mesén del ICE, se localiza la certificación DTIC-2011-2020 de fecha 06 de abril de 2020 emitida por la Dirección de Tecnologías de Información y Comunicaciones y dirigida al ICE en los siguientes términos:*

*"Los suscritos Robert Picado Mora, cédula 1-0843 0020, en calidad de Subgerente de la Dirección de Tecnologías de Información y Comunicaciones, Christian Chacón Rodríguez, cédula 1-0906 0472, en calidad de Subdirector de la Dirección de Tecnologías de Información y Comunicaciones y Sergio Porras Solís cédula 3-0310 0598, en calidad de Jefe del Área de Comunicaciones y Redes Informáticas, de la Dirección de Tecnologías de Información y Comunicaciones de la Caja Costarricense de Seguro Social (CCSS), certificamos que actualmente* ***el core de comunicaciones del Centro de Datos corresponde a Tecnologías Cisco****, esa tecnología considera el Centro de Datos CODISA, el Centro de Comunicaciones del piso 11, y el alcance de esa plataforma incluye las redes LAN de esos sitios, los componentes de WAN entre ellos y la interconexión a todos los sitios Caja." (El resaltado no es del original)*

*En ese sentido, se instruye a la DTIC para que atienda como en derecho corresponde lo dispuesto por parte de la Junta Directiva mediante acuerdo tercero del artículo 132 de la sesión 9189; para ello* ***deberá garantizar que las bases de la contratación atiendan los diversos principios que cobijan a la contratación administrativa y no se incorporen disposiciones que puedan entenderse como direccionamientos a marcas específicas****, sino que deberán referenciarse los atributos técnicos requeridos de los bienes y servicios objeto de la contratación en razón de su funcionalidad, operabilidad, interoperabilidad o cualquier otro atributo técnico necesario, conforme a los estudios técnicos previos que se realicen o hayan realizado, los cuales fundamentaran tanto la excepción que se utilizará como la adquisición de fondo que se efectúa.*

*Por último, se recuerda que el propiciar un efectivo cumplimiento al principio de libre concurrencia – eliminando cualquier direccionamiento del concurso en cuestión – no representa un mero formalismo que debe ser atendido para cumplir con la norma, sino que eficientiza la gestión de abastecimiento, para el caso en cuestión, potenciaría la participación de múltiples fabricantes, aspectos que podría ayudar a una mayor diversificación en las ofertas y eventual reducción de costos con un mismo resultado en el servicio informático ofrecido."*

En consonancia con lo anterior, el Ing. Roberto Blanco Topping, subgerente a.i, mediante oficio GG-DTIC-2022, del 25 de febrero de 2022, solicitó al Máster Danilo Hernández Monge, subdirector a.i, ambos de la DTIC, de conformidad con la instrucción recibida por la Gerencia General, proceder con la revisión de los criterios técnicos que fueron presentados a la Junta Directiva para que se determine si estos responden a una sana aplicación de los principios de contratación administrativa, para lo cual se debe conformar un equipo de trabajo que se aboque a la revisión de lo actuado desde el punto de vista técnico y que realice las acciones necesarias que permitan dar continuidad al proyecto, en un plazo máximo de dos meses.

## I.III PRODUCTOS DE AUDITORÍA INTERNA RELACIONADOS CON SITIO ALTERNO DE PROCESAMIENTO DE DATOS

En relación con la implementación del sitio alterno esta Auditoría ha emitido múltiples productos señalando diversas oportunidades de mejora previo a la materialización de los riesgos evidenciados en el ciberataque del 31 de mayo de 2022, según se detallan seguidamente:

**Informes de Auditoría:**

**ATIC-461-2012:** Se identificaron oportunidades de mejora relacionadas con la gestión de la seguridad de la Plataforma Tecnológica, específicamente en temas como el desarrollo de un estudio de vulnerabilidad informática, espacio físico del cuarto de servidores, seguridad física del Área de Gestión Informática, así como el mantenimiento de la planta eléctrica y la Unidad Ininterrumpida de Potencia (UPS) del Edificio Jorge de Bravo, así como la vigencia del Contrato de servicios de mantenimiento de la Plataforma Tecnológica Central de la Gerencia de Pensiones.

**ATIC-196-2013:** Se constató oportunidades de mejora en aras de lograr a continuidad de la prestación de los servicios, a través del fortalecimiento de aspectos como el contrato de mantenimiento de la Plataforma Tecnológica Central y la oficialización del Plan de Continuidad de Tecnologías de Información y Comunicaciones. Aunado a esto, se determinó que la institución no dispone de un sitio alterno como contingencia en caso de presentarse algún evento que interrumpa de manera prolongada los servicios que se brindan.

Por otro lado, actualmente el Core de equipos de comunicaciones Institucional se hospeda en el piso 11 del Edificio Genero Valverde, esto a pesar de que la Caja dispone de un Centro de Cómputo Principal certificado para albergar los equipos que conforman la Plataforma Tecnológica Central.

**ATIC-21-2014:** Se determinó la ausencia de un contrato de servicios de mantenimiento de la Plataforma Tecnológica Central y de planes de contingencia que brinden seguridad razonable de la capacidad de respuesta institucional ante la materialización de riesgos.

**ATIC-154-2014:** Los resultados del estudio efectuado permitieron evidenciar que se presentan oportunidades de mejora de control interno en los procesos para garantizar la continuidad en la prestación de los Servicios de Tecnologías de Información y Comunicaciones que brinda el CCP. Lo anterior, por cuanto la institución aún no define y aprueba una estrategia para disponer del servicio de hospedaje para el centro de cómputo principal institucional a largo plazo.

Además, se determinó que la Sala TIER II del CCP se encuentra utilizada en un 75% de su capacidad, situación que podría ir en detrimento con las finanzas institucionales si se considera el monto pagado por el arrendamiento de dicho espacio. Además, no se dispone de un procedimiento oficial que establezca los requerimientos técnicos que deben tener los equipos de tecnologías de información y comunicaciones (TIC) para ser hospedados en el CCP, así como el tipo de información y servicios que operan en dichos dispositivos.

**ATIC-45-2016:** se destacó la necesidad que la CCSS valore la inversión en nuevas herramientas para el fortalecimiento de la seguridad en la plataforma técnica, considerando métricas expuestas por la empresa Gartner en donde se recomienda destinar al menos un 6% del presupuesto total de las organizaciones en ese sentido. Otro aspecto señalado refiere a la suficiencia de recurso humano suficiente y competente en esa materia, así como definición de políticas y normativas actualizadas y alineadas al marco regulatorio establecido por la Contraloría General de la República, y finalmente, la importancia sobre la aplicación de indicadores orientados a alertar oportunamente sobre el límite de accesos a las aplicaciones institucionales, detección de comportamientos irregulares en el uso de sistemas de información y afectaciones al rendimiento de herramientas tecnológicas, entre otros.

**ATIC-51-2016:** Implementación de la Etapa I del Proyecto de Fortalecimiento de la Infraestructura Tecnológica Principal. Los resultados del estudio efectuado respecto de las acciones adoptadas por la Administración Activa para ejecutar dicha iniciativa han permitido evidenciar que se presentan oportunidades de mejora de control interno en las actividades de definidas para la adquisición, instalación y puesta en funcionamiento de los equipos de Tecnologías de Información y Comunicaciones (TIC) adquiridos mediante la licitación N° 2015LN-000012-05101 para remozar la Plataforma Tecnológica Central.

**ATIC-059-2016:** Evaluación sobre la gestión de Producción en Sistemas y Servicios de Tecnologías de Información (TI) efectuada por el Área de Soporte Técnico, específicamente en la Subárea Gestión de Producción.

Se determinaron debilidades referentes al cumplimiento de los lineamientos establecidos por la DTIC para el desarrollo de documentos asociados a los procesos de trabajo en la Subárea Gestión de Producción, tales como: gestión de monitoreo y respaldos de la información en la Plataforma Tecnológica Central.

**ATIC-026-2017:** Avance del Proyecto de Fortalecimiento de la Infraestructura Tecnológica Principal.

Se comprobó que durante los últimos siete años se han identificado riesgos asociados a la continuidad de los servicios del Centro de Cómputo Principal (CCP) y a la fecha de elaboración del presente informe, no han sido mitigados en su totalidad, entre los que destaca la oficialización e implementación de una estrategia para disponer de un Centro de Datos Principal y Sitio Alterno para contingencias en el tiempo.

Se identificó que el contrato No. 004-2009 suscrito entre la Caja Costarricense de Seguro Social y la empresa Ideas Gloris S.A para el "Servicio para hospedaje para albergar el Centro de Cómputo Principal de la CCSS" finalizaba en agosto del 2017, lo cual podría ocasionar la interrupción indefinida de servicios médicos, financieros y de pensiones dependientes de la operativa de sistemas de información críticos tales como el Sistema Centralizado de Recaudación (SICERE) y el Expediente Digital Único en Salud (EDUS).

Según se desprendió del Estudio Preliminar y Factibilidad del Proyecto de Fortalecimiento de la Infraestructura Tecnológica Principal, la Administración había analizado cuatro alternativas para habilitar el Centro de Datos Principal y Sitio Alterno, sin embargo, no se había definido las condiciones en las cuales se prestarían dichos servicios (Acuerdos de Servicio), los servicios que serían trasladados a esos recintos, así como las funciones del personal que administra el CCP, lo cual podría materializar riesgos inherentes al uso de recursos públicos, debido a que el nuevo Centro de Datos Principal se pretende arrendar bajo la modalidad de demanda de servicios y el proveedor del servicio asumiría su administración.

**ATIC-76-2018:** Evaluación sobre la gestión de las telecomunicaciones a nivel institucional.

Los resultados del estudio evidenciaron oportunidades de mejora en la administración de la plataforma tecnológica utilizada para las telecomunicaciones, en aspectos como el cumplimiento de las funciones establecidas en el marco normativo aplicable, así como la necesidad del uso eficaz y eficiente de las tecnologías de manera integral para alcanzar el cumplimiento de la estrategia plasmada por la Caja Costarricense del Seguro Social.

Adicionalmente, en el informe **ATIC-166-2020**, "Auditoría de carácter especial sobre la gestión integral de la plataforma tecnológica central", específicamente en el hallazgo 1 "Sobre el sitio alterno de procesamiento de datos", se indicó:

> *"Esta Auditoría constató que, al 30 de noviembre del 2020, la Institución no dispone de un sitio alterno al Centro de Datos Principal para la operación de sistemas y servicios.*
>
> *Lo anterior, resulta relevante por cuanto han transcurrido aproximadamente seis años desde la celebración de la sesión N°8751, donde la Junta Directiva determinó a través del artículo N°10 que se presentara una propuesta de solución en el caso particular de la Plataforma Tecnológica Central y el Sitio Alterno.*
>
> *Por otra parte, en el documento denominado "Informe de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), para Junta Directiva" de octubre del 2020, se desarrollaron ocho alternativas, en las cuales se proponen los siguientes escenarios:*
>
> - *La contratación de las instalaciones ubicadas en CODISA como Sitio Principal o Alterno en seis oportunidades.*
> - *La construcción de un Centro de Datos Principal propiedad de la Caja Costarricense del Seguro Social en cuatro propuestas, no obstante, en el 2018, la Presidencia de la República, el Ministerio de Hacienda y el Ministerio de Ciencia, Tecnología y Comunicaciones (MICIT), mediante la directriz "Mejoras en la eficiencia del gasto público mediante el uso adecuado de tecnologías digitales en el sector público costarricense, específicamente en el artículo N°2, instruyeron a las instituciones del Estado no iniciar nuevos procesos de construcción de centros de datos o "Datacenters".*
> - *La incorporación de nubes públicas como solución para el Centro de Datos Principal y el Alterno en dos alternativas. La Contratación del Centro de Procesamiento Alterno por servicios con el ICE en el desarrollo de las dos últimas propuestas.*
> - *El mejoramiento de la infraestructura del Centro de Comunicaciones en Oficinas Centrales es valorado en uno de los escenarios definidos por la DTIC."*

En consonancia con lo anterior el Máster Christian Chacón Rodríguez, en ese momento[3] subdirector de Tecnologías de Información y Comunicaciones al respecto mencionó:

> *"Actualmente no tenemos un sitio alterno y es un riesgo, en temas de ofertas hemos tenido desde las primeras por $140 000 000 hasta $12 000 000, ya que hemos acotado mucho los sub-ítems. Lo anterior debido a la necesidad de habilitar un sitio contingente que nos permita direccionar los servicios en caso de una emergencia.*

[3] Entrevista efectuada el 19 de octubre de 2020, informe ATIC-166-2020

*Aunado a esto, se deben definir los roles y responsabilidades con la correspondiente capacitación para administrar dos centros de datos, el establecimiento del encargado del negoció a cargo de tomar la decisión en torno al momento de efectuar el traslado al sitio alterno y al sitio principal, por lo tanto, no es solamente habilitar capacidad tecnológica."*

Aunado a lo anterior, el Máster Jorge Sibaja Alpízar, jefe del Área de Soporte Técnico, mencionó[4] lo siguiente:

*"Actualmente no tenemos sitio alterno, en caso de que se presente una falla o eventualidad en CODISA nos quedaríamos sin servicios, lo anterior porque lo que tenemos en oficinas centrales son respaldos, por ejemplo, estamos replicando la base de datos de SICERE íntegra en comparación de la utilizada en producción, así como la del EDUS y otros repositorios de información complementarios para utilizar ciertos servicios. En caso de una falla de estas bases de datos en CODISA, podrían utilizarse, las de piso 11, oficinas Centrales, contingentemente. Pero es una contingencia parcial.*

*En ese mismo orden de ideas, en caso de que se apague el Data Center ubicado en CODISA los servicios prestados a través de aplicativos como EDUS, SICERE, MISE y Presupuesto dejarían de funcionar. Por otra parte, tenemos elementos complementarios por ejemplo si la base de datos de EDUS o SICERE se desconectaran en el Data Center podemos conectarnos a la del piso 11. De hecho, se hace con EDUS, cuando debe darse mantenimiento a SICERE, los servicios que EDUS requiere a SICERE lo usa de la base de datos Replicada de SICERE en Oficinas centrales.*

*Por lo cual, no podemos decir que tenemos sitio alterno como tal. De hecho, por parte de la dirección se han realizado diversas propuestas y el tema se encuentra en Junta Directiva pero todavía no ha avanzado.*

*Existe una propuesta de sitio alterno y debería de aprobarla el negocio que debe considerar que es crítico, por lo cual hay que invertir tanto en protegerlo."*

Finalmente, el Máster Alexander Ordoñez Arroyo, jefe de la Subárea de Administración de Plataformas, mencionó[5] lo siguiente:

*"Sobre el tema de contingencia, actualmente la CCSS no tiene Sitio Alterno oficial por eso no hay simulacros. En este momento lo que tenemos es una pequeña replica de ciertos componentes en el piso 11 del edificio Jenaro Valverde Marín."*

Aunado a lo anterior, en el apartado "Conclusiones", esta Auditoría indicó:

*"En lo que respecta a la definición del Sitio Alterno al Centro de Datos Principal ubicado actualmente en el Parque Tecnológico de CODISA,* ***resulta relevante seleccionar la alternativa a desarrollar con el objetivo de disponer el lugar donde se albergaría la infraestructura tecnológica tanto principal como secundaria, con el fin de brindarle continuidad y disponibilidad de los servicios ante alguna contingencia****.*

*Aunado a esto, se identificó la necesidad de efectuar simulacros y pruebas de manera integral, considerando los actores del negocio y los especialistas en TIC para verificar el adecuado funcionamiento del Plan de Continuidad de los servicios prestados a través de la disponibilidad de la Plataforma de marras, así como la posibilidad de que la Institución valore su capacidad de respuesta ante eventos en dispositivos de hardware y/o software de la PTC, entre otras circunstancias que se puedan presentar.*

[4] Entrevista efectuada el 9 de setiembre de 2020, informe ATIC-166-2020
[5] Entrevista efectuada el 9 de octubre de 2020

*Finalmente, en relación con la adquisición de servicios de hospedaje del Centro de Datos Principal y posterior al análisis de las alternativas propuestas por la Dirección de Tecnológicas en torno a la definición del Sitio Principal y su respectivo Alterno, es necesario se valoren, entre otros, los riesgos asociados a la contratación de terceros.*

*Asimismo, es preciso se valore la eventual dependencia con la empresa Gloris S.A y posibles escenarios para el funcionamiento de los centros de procesamiento de datos de la Institución." (lo resaltado no corresponde al original).*

Finalmente, se emitió la siguiente recomendación:

***"RECOMENDACIONES***

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

*2. Hacer de conocimiento del Consejo Tecnológico como la instancia de nivel superior responsable de la toma de decisiones estratégicas y seguimiento de los temas relacionados con tecnologías de información y comunicaciones, sobre los siguientes aspectos relacionados con la gestión de la PTC:*

1. *Antecedentes relacionados con la valoración de los escenarios para el hospedaje y procesamiento del Sitio de Cómputo Principal y Alterno de la PTC.*

2. *Análisis de Factibilidad realizado a cada alternativa, así como la gestión de riesgos identificados.*

3. *Recomendación de la alternativa a criterio de la Dirección de Tecnologías de Información y Comunicaciones justificando los criterios utilizados en ese sentido.*

4. *Estado de la Licitación Pública 2017LN-000001-1150 "Servicio de Hospedaje para Albergar el Centro de Cómputo Principal.*

5. *Valoración de los riesgos asociados.*

*Lo anterior, con el fin de seleccionar la propuesta más viable técnica, financiera, operativa y jurídica para su implementación en la Caja Costarricense de Seguro Social, considerando criterios de eficiencia, eficacia y sana administración.*

*Posterior a la selección de la alternativa, presentar a ese Consejo, una propuesta del conjunto de iniciativas que permitan la puesta en marcha de su implementación, en alineamiento con el Modelo Meta de Gobernanza de las TIC y la Seguridad de la Información y la AGEDI. Para lo anterior, es importante considerar el plazo transcurrido desde la identificación de la necesidad asociada al tema citado en la presente recomendación.*

*Para acreditar el cumplimiento de esta recomendación, debe remitirse a esta Auditoría en un plazo de cuatro meses a partir de la fecha de recepción del presente informe, la documentación que respalde las acciones ejecutadas por esa Dirección para la definición de la alternativa del Centro de Procesamiento de Datos Principal y su respectivo Sitio Alterno, así como la aprobación del conjunto de iniciativas para su implementación."*

A efectos de verificar el avance en el cumplimiento de la recomendación mencionada se emitió seguimiento **SATIC-20-166-01-2022**, del 18 de marzo del 2022, en el cual se consideró la recomendación en estado **"En Proceso"**, dado que a esa fecha no se había concretado la definición de una alternativa del Centro de Procesamiento de Datos Principal y su respectivo Sitio Alterno, asimismo, no se evidenció la participación del Consejo Tecnológico como la instancia de nivel superior responsable de la toma de decisiones estratégicas y seguimiento de los temas relacionados con tecnologías de información y comunicaciones, cuya participación se considera fundamental para concretar este proyecto y así fortalecer la continuidad de las actividades sustantivas de la institución ante las eventuales (en ese momento) interrupciones provocadas por desastres naturales, problemas de funcionamiento de dispositivos, vulnerabilidades de seguridad entre otros.

Adicionalmente, en el mencionado seguimiento, se indicó:

> *"Por su parte, si bien es cierto, queda evidenciado que desde el acuerdo adoptado por la Junta Directiva (artículos 18° de la sesión 8768 del 19 de marzo 2015; 13° de la sesión 8821 del 21 de enero 2016 y 38° de la sesión 8831 del 10 de marzo 2016), relacionados con el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), la administración activa ha venido realizando acciones en procura del fortalecimiento de la infraestructura tecnológica principal, ejemplo de ello queda constando en los oficios:*
>
> - *Oficio DTIC-1368-2017 del 10 marzo 2017, Primer informe de avance del 2017 sobre el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos).*
> - *Oficio DTIC-4867-2017 del 16 de agosto 2017, Segundo Informe de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), para Junta Directiva.*
> - *Oficio DTIC-2187-2019 del 01 de abril 2019, informe a la Gerencia General, dada la disposición de la Junta Directiva del 21 de marzo 2019, del traslado de la Dirección de Tecnologías de Información y Comunicaciones a depender jerárquicamente de la Gerencia General.*
> - *Oficio DTIC-7943-2019 del 11 de diciembre 2019, Primer informe trimestral avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), para Junta Directiva.*
> - *Oficio DTIC-2174-2020 del 16 de abril 2020, Certificación sobre el Core de Comunicaciones del Centro de Datos Caja Costarricense de Seguro Social.*
> - *Oficio GG-DTIC-4140-2020 del 16 de julio 2020, actualización de propuesta preliminar técnico-comercial de estudio de mercado del Servicio Administrado para el fortalecimiento de la Infraestructura Redundante para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA) para la Caja Costarricense de Seguro Social.*
>
> *Asimismo, la Junta Directiva en la sesión 9189, artículo 132° del 24 de junio 2021, dispuso:*
>
> ***ARTICULO 132º***
>
> *Se conoce oficio N° GG-DTIC-2432-2021, de fecha 6 de mayo de 2021, suscrito por el Ing. Roberto Blanco Topping, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones mediante el cual presenta el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (centro de datos)*

*Solicitud para que la Junta Directiva brinde aval a la estrategia propuesta para implementar la Alternativa #8 del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos Principal y Centro de Datos Alterno) y se apruebe para que la Dirección de Tecnologías de Información y Comunicaciones inicie el proceso de contratación directa con Instituto Costarricense de Electricidad mediante la excepción entre entes de derecho público. (…)*

***ACUERDO SEGUNDO:***

*Aprobar la estrategia propuesta para implementar la Alternativa #8 del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos Principal y Centro de Datos Alterno).*

***ACUERDO TERCERO:***

*Se Instruye a la Dirección de Tecnologías de Información y Comunicaciones para que inicie el proceso de contratación directa con el Instituto Costarricense de Electricidad mediante la excepción entre entes de derecho público."*

Finalmente, se consideró en el seguimiento en mención, que la Dirección de Tecnologías de Información y Comunicaciones había realizado gestiones relacionadas con la disposición de Junta Directiva, según se reflejan en los siguientes oficios:

- Oficio GG-DTIC-4823-2021, con fecha 25 de agosto 2021, designación de la comisión técnica a cargo del análisis de ofertas y recomendación de adjudicación de la compra "Solución para el fortalecimiento de la Infraestructura Redundante de Procesamiento de Información para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA)", la cual está conformada por los siguientes funcionarios: Ing. Geiner Gamboa Otárola, Ing. Sergio Porras Solís, Ing. Jeannette Madrigal Loría, Ing. Wilfredo Porras Morales, Ing. Olger Vargas Pérez, Ing. Esteban Gonzalez Monge, Ing. Adrián Madrigal Gómez, Ing. Roger Palavicini Villalobos, Ing. Vanessa Carvajal Carmona, Ing. Erick Vindas Umaña, Ing. Michael Leandro Fuentes y Lic. Endry Núñez Salas.

- Oficio GG-DTIC-4665-2021, del 18 de agosto 2021, se envió al ICE las especificaciones técnicas como insumo para la oferta formal por parte del ICE.

- Oficio GG-DTIC-6882-2021 del 18 de noviembre 2021, Respuesta a oficio GG-DTIC-6165-2021, sobre Informe y estudios realizados para la escogencia de alternativa No. 8, Proyecto Sitio Alterno.

- Oficio GG-DTIC-7431-2021, del 14 de diciembre 2021, solicitando instrucción a la gerencia general, sobre la adquisición del Servicio Administrado para el fortalecimiento de la infraestructura redundante del Centro de Procesamiento Primario (CPP) y el Centro de Procesamiento Alterno (CPA) de la Caja Costarricense de Seguro Social (CCSS)

- Oficio GG-DTIC-0194-2022, del 12 de enero 2022, remisión criterio del área de la SGA-DTIC, sobre "Observaciones a solicitud de contratación".

**Oficios de Auditoría**

Adicionalmente, se han emitido oficios en los cuales se advierte de los riesgos vinculados con esta materia, según se detalla seguidamente:

- **Oficio AD-ATIC-38000-2014:** Oficio de advertencia relacionado con la "Finalización del Contrato 004-2009 "Servicio de hospedaje para albergar el Centro de Cómputo Principal (CCP) de la CCSS", vinculado con la importancia de disponer del servicio de hospedaje para albergar el Centro de Cómputo y la continuidad de los servicios brindados por la institución.

- **Oficio 65500-2016:** Oficio relacionado con la Propuesta acto de Re-Adjudicación Licitación Pública 2015LN-000012-05101" Reforzamiento de la Plataforma Tecnológica Institucional", en el que se efectuaron diversas observaciones asociadas al establecimiento de una solución definitiva para el Centro de Cómputo Principal que permita la continuidad en la prestación de los servicios tecnológicos brindados de manera razonable.

- **Oficio AD-ATIC-49167-2017:** Oficio de Advertencia sobre la Finalización del Contrato 004-2009 "Servicio de hospedaje para albergar el Centro de Cómputo Principal (CCP) de la CCSS", referente al contrato 004- 2009 suscrito entre la Caja Costarricense de Seguro Social y la empresa Ideas Gloris S.A. para el "Servicio para hospedaje para albergar el Centro de Cómputo Principal de la CCSS."

- **Oficio AD-ATIC-5021-2018:** Oficio de advertencia sobre la vigencia actual de plataforma tecnológica Institucional y la calidad de la información almacenada en el Sistema Contable Bienes Muebles de la Caja Costarricense de Seguro Social, con énfasis al porcentaje de depreciación en los equipos que conforman la plataforma tecnológica de la Institución, además de analizar un muestreo de los registros del Sistema Contable Bienes Muebles, a fin de verificar la integridad, confiabilidad y oportunidad de los datos.

## II. ESTADO DE SITUACIÓN DEL SITIO ALTERNO DE PROCESAMIENTO DE DATOS AL MOMENTO DEL CIBERATAQUE DEL 31 DE MAYO DE 2022.

Mediante oficio GG-DTIC-2633-2022, del 23 de mayo de 2022, el Ing. Roberto Blanco Topping, subgerente a.i, comunicó a esta Auditoría, en lo que interesa:

> ***"Tercero, es correcto que la DTIC no cuenta hoy con un centro de datos alterno de procesamiento donde en caso de que se den eventos que pudieran inhabilitar el acceso o los servicios mismos, se pueda dar continuidad a las operaciones prestadas. Al respecto de este tema, debemos ser claros que no en todos los casos el contar con un sitio alterno puede ser la solución a una situación como las referidas (AD-ATIC-038-2022)*** *y en atención, ya que en general, las plataformas deben estar interconectadas entre sí para poder mantener la actualización en tiempo real de los datos, y propiciar la disponibilidad de los servicios, y la red debe estar habilitada para brindar el acceso hacia cualquiera de los puntos habilitados como sitios de prestación.*
>
> *Es obvio que, en otras muchas situaciones, como: incendio en el sitio, falla de los equipos de procesamiento, almacenamiento, comunicaciones, balanceo, seguridad, Aires acondicionados, Unidades de Potencia ininterrumpida, proveedor de comunicaciones, Mantenimiento Críticos, delitos internos, etc. Y en algunas circunstancias desastres naturales, el contar con al menos un segundo sitio, será la solución para mantener la disponibilidad de los servicios, y por ello, la DTIC dentro de sus múltiples labores, capacidades y limitaciones, dio continuidad al proceso instruido por la Junta Directiva (…)". (lo resaltado corresponde al original)*

Con la finalidad de verificar el estado de situación relacionada con el establecimiento de un sitio alterno de procesamiento de datos al momento del ciberataque se sostuvo reunión el 14 de junio del 2022, por medio de la plataforma institucional de videollamadas TEAMS con el Máster Danilo Hernández Monge, subdirector a.i de Tecnologías de Información y Comunicaciones, quien indicó que a la fecha no se cuenta con un sitio alterno para el procesamiento de datos, debido entre otros factores a la ausencia de definición institucionalmente del modelo y/o alcance requeridos, así como de las expectativas de solución que se aportarían a la continuidad de los servicios.

Aunado a lo anterior, el Máster Hernández Monge, señaló que posterior al acuerdo de Junta Directiva se procedió a la elaboración de documentación con la finalidad de sustentar el procedimiento de compra, la cual fue remitida a la Sub Área de Gestión de Compras de la DTIC, quienes hicieron observaciones a efectos de fortalecerlo, a ese momento se había establecido un grupo de trabajo técnico y se encontraba en la fase final de la revisión de las observaciones mencionadas y se esperaba el momento idóneo para presentar en sesión interna de trabajo los resultados de la valoración efectuada.

Además, el Máster Hernández Monge señaló la importancia de acotar y aclarar el alcance del proyecto a implementar dado que en caso de efectuarse la inversión requerida con la finalidad de asegurar la continuidad solamente de algunos servicios, se podrían generar posteriormente cuestionamientos relacionados con aquellos no estén incluidos en este proyecto.

De forma tal, según lo indicado por el Máster Hernández Monge, se requiere de un proceso de análisis mayor que permita con claridad establecer con la participación de todos los niveles institucionales, cuáles son las expectativas del sitio alterno, en cuanto a la respuesta en la continuidad de los servicios y sistemas críticos para el funcionamiento de la institución al momento de presentarse una situación de afectación y se tenga claridad de cuales serán recuperados mediante este mecanismo.

Adicionalmente, el Máster Hernández Monge señaló que la definición mencionada anteriormente resulta importante desde la perspectiva de la inversión para la solución a implementar, si la dimensión es la de duplicar todos los servicios que provee el sitio principal y la institución pueda funcionar sin afectaciones tecnológicas ante una eventualidad, requeriría un nivel de costos similares a los actuales en aspectos tales como licencias, alojamientos, plataforma, entre otros.

Además, los costos varían de acuerdo con el modelo a implementar, sea esta la duplicación del sitio principal o la recuperación de los sistemas y servicios que se consideren críticos u otras alternativas para permitir la operación institucional en tanto se ejecutan los procedimientos y protocolos para recuperarse ante la materialización de una eventualidad.

## III. CONSIDERACIONES

En consonancia con lo anterior, ya sea por cumplimiento normativo, tendencia de mercado, mejor práctica mundial, o planificación de continuidad de negocio, es vital para organizaciones en general y más aún para la CCSS como institución encargada de la prestación de servicios de salud y pensiones a los ciudadanos del país, disponer de un sitio alterno de procesamiento de datos como parte de la infraestructura de tecnologías de información, de manera que se brinde la posibilidad de minimizar riesgos asociados a la interrupción de servicios al afectarse el sitio principal, tal como ocurrió a partir de la desconexión de sistemas efectuada el 31 de mayo del 2022 en forma preventiva ante al ataque cibernético sufrido en la Institución, lo anterior en aras de garantizar razonablemente la continuidad de operación de sistemas y servicios tecnológicos, así como el establecimiento de medidas contingentes.

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."*

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 XIII "Continuidad y Disponibilidad de los Servicios Tecnológicos", establece:

> *"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos,* ***la recuperación ante un desastre y la respuesta ante incidentes****, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
>
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción." (lo resaltado no corresponde al original)*

De conformidad con el nivel de automatización de los servicios, lo que implica un mayor desarrollo de sistemas, así como de un constante crecimiento en el volumen de información de diversos ámbitos en los cuales se desempeña la institución, y en virtud de la materialización del riesgo como resultado del ciberataque que tuvo efecto en la operación de las aplicaciones informáticas, resulta de vital importancia concretar los esfuerzos iniciados con la finalidad de dotar a la institución de un sitio alterno de procesamiento de datos, que permita asegurar al menos el funcionamiento mínimo de aquellos elementos que se consideren de carácter crítico ante una interrupción.

En ese orden de ideas, debe definirse con claridad, tanto el modelo como el alcance de esta herramienta, así como los protocolos para su funcionamiento, dentro de las estrategias de manejo de crisis que en su momento disponga la institución, así como su ubicación en los planes de continuidad, contingencia y recuperación que se desarrollen.

Lo anterior, considerando la revisión de los antecedentes y estado actual del proyecto de dotación de este elemento, así como la conformación de los equipos de trabajo a cargo de su desarrollo e implementación.

Adicionalmente, verificar el cumplimiento de la normativa administrativa y técnica correspondiente mediante la oportuna participación de los entes asesores y de dirección institucionales, con la finalidad de asegurar su implantación correcta en la infraestructura tecnológica.

De forma tal, las observaciones emitidas en el presente oficio, así como en los diversos productos emitidos por este Órgano de Fiscalización y Control, en los cuales se incluyen oportunidades de mejora para minimizar los riesgos advertidos sobre la necesidad de contar con un sitio alterno de procesamiento de datos, tienen como objetivo la generación de esfuerzos articulados y consistentes para la recuperación ante los eventos que provoquen una interrupción de los servicios.

En virtud de lo expuesto, se previene y advierte a esa Administración con el propósito de que se adopten las medidas pertinentes, a fin de ejecutar las acciones que correspondan, con la finalidad de dotar a la institución de un sitio alterno de procesamiento de datos, las cuales deben ser sometidas a valoración y revisión según corresponda.

Lo anterior, con el objetivo de enfrentar con éxito los eventos adversos que puedan presentarse, así como coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para la recuperación de los servicios afectados por el impacto ante la interrupción materializada por el ataque sufrido, por otros riesgos ya identificados o eventos de carácter imprevisto.

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 dos meses** a partir del recibido de este documento.

Atentamente,

**AUDITORÍA INTERNA**

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.13 13:39:29 -06'00'

Lic. Olger Sánchez Carrillo
**Auditor**

OSC/RJS/RAHM/AAM/lbc

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva – 1102.
Auditoría