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

AS-AATIC-194- 2022
4 de octubre de 2022

Licenciado
Jaime Barrantes Espinoza, gerente

Ingeniero
Marco Vinicio González Jiménez, jefe
Centro de Gestión Informática
GERENCIA PENSIONES - 9108

Estimados señores:

ASUNTO:	**Oficio de Asesoría referente al sitio alterno de procesamiento de datos de la Gerencia de Pensiones, 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 el sitio alterno de la Gerencia de Pensiones ubicado en el sitio principal de procesamiento de datos institucional (CODISA), suspendido de manera preventiva a raíz de los ataques cibernéticos sufridos por la institución el pasado 31 de mayo del 2022.

En consonancia con lo anterior, esta Auditoría en complemento del oficio AD-AATIC-078-2022 del 13 de julio de 2022, en el cual se advertía a la administración sobre la urgente necesidad de disponer de un centro alterno de procesamiento de datos, consultó al Lic. Marco González Jiménez, jefe a.i del Centro de Gestión Informática de la Gerencia de Pensiones sobre la condición actual de este elemento en la infraestructura de tecnologías de información y comunicaciones de esa gerencia.

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 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.

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 de 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 declaratoria de estado de emergencia institucional por los ciberataques, en lo que interesa indicó:

> *"(…)*
>
> *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)."*

En virtud de lo anterior, se comunicaron afectaciones en los procesos que se ejecutan en la Gerencia de Pensiones, los cuales fueron documentados por medios de comunicación de alcance nacional, entre los más relevantes se encuentran:

- Diario La Nación, 1 de junio 2022 "Hackeo obliga a CCSS a ampliar plazo para que patronos presenten planillas de mayo. Nueva fecha límite es el 10 de junio. Extensión es parte de las medidas de contingencia debido al ataque cibernético del martes en la madrugada".

- Diario La Nación, 4 de junio 2022 "Libre trasferencia entre operadoras de pensiones queda suspendida por hackeo a la CCSS".

- Diario digital CrHoy, 6 de junio 2022, "CCSS sigue con problemas para pagar incapacidades".

- Diario digital La República, 6 de junio 2022, "Patronos y trabajadores independientes atrasados por hackeo no serán multados".

- Diario La Nación, 7 de junio 2022, "Hackeo de la Caja paraliza entrega de nuevas pensiones del IVM y ROP".

- Diario digital CrHoy, 13 de junio 2022, "CCSS amplía periodo de presentación de planillas por afectación de hackeo".

- Diario La Nación, 13 de junio 2022, "Hackeo a CCSS impedirá pagar aumento a pensiones del IVM en junio".

- Semanario Universidad, 17 de junio 2022, "Caja reactivará la próxima semana plataforma SICERE para recaudación en línea".

Es conveniente indicar que los servicios brindados por la Gerencia de Pensiones fueron paulatinamente recuperados.

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

Los servicios que presta la institución son de vital importancia dado su relación directa con la salud de los costarricenses, así como su bienestar en la etapa correspondiente al disfrute de la pensión posterior a su salida del mercado laboral o por afectaciones sufridas en su capacidad laboral, de forma tal, resulta necesario la implantación de mecanismos que permitan garantizar su continuidad, tales como planes de contingencia, de continuidad, de recuperación del negocio, entre otros.

En ese contexto, con la finalidad de evitar las interrupciones en el negocio deben identificarse con claridad los riesgos a los que se expone la organización en los diversos procesos y procedimientos que se ejecutan para satisfacer las necesidades de los asegurados. Aunado a lo anterior, se requiere de la determinación de los niveles de criticidad de las herramientas, aplicaciones, equipos, sistemas y demás componentes de la infraestructura tecnológica institucional, permitiendo establecer cuales elementos requieren de continuidad permanente con la finalidad de no detener la marcha habitual y las prestaciones diarias.

Dentro de ese marco, un sitio alterno de procesamiento de datos requiere de las definiciones anteriores, dentro de un ambiente que permita dar continuidad a las tareas de mayor importancia y criticidad del negocio en caso de materializarse una interrupción o suspensión de los servicios que presta el sitio principal[1], incluyéndose entre otros elementos los respaldos de bases de datos, los sistemas, las herramientas tecnológicas y aquellos elementos necesarios para iniciar las operaciones de acuerdo con los protocolos establecidos en los planes de contingencia y continuidad, dependiendo su efectividad de la compatibilidad con el sitio principal.

De forma tal, el sitio alterno[2] se define como un elemento de infraestructura tecnológica que se mantiene listo para su uso durante o posterior a un evento que comprometa la continuidad del negocio a efectos de asegurar la prestación de los servicios críticos. Este concepto tiene variantes en su capacidad, alcance y tiempo de respuesta, así puede desarrollarse desde un sitio “espejo” totalmente redundante e idéntico al principal, donde la información se refleja en tiempo real, está configurado y contiene el equipamiento, software y herramientas necesarias para operar en sustitución del principal. En contrario puede establecerse un sitio alterno que consideren únicamente el funcionamiento de aquellos elementos críticos para la prestación de los servicios.

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 representa una mayor inversión por su nivel de complejidad, no obstante, se continuaría la prestación con una afectación mínima, en contrario al disminuir los elementos que soporta el monto es menor, así como los elementos a los que se daría continuidad.

[1] El sitio principal de procesamiento de datos es el ambiente en el cual se alojan los recursos informáticos que soportan el negocio, cuenta con los elementos necesarios para que la organización cumpla con sus objetivos y provee los medios necesarios para la operación cotidiana.
[2] Fuente: Sitio alterno https://www.openriskmanual.org/wiki/Alternate_Sitetivo - Manual de riesgo abierto (openriskmanual.org)

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

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 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:

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

Alternativa	Descripción	Sitio Principal	Sitio Alterno	Precio Menor	Precio Mayor
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).	$37.308.768	$63.342.144
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).	$49.561.671	$78.364.463
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. • Operación de equipos por leasing a demanda. • Contratación de servicios de administración, mantenimiento y operación.	$86.870.439	$141.706.607
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. • Adquisición de equipamiento tecnológico. • Contratación de servicios de administración, mantenimiento y operación.	$47.657.600	$74.612.479
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).	$38.316.478	N/A
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. • Mejoras en la infraestructura del Centro de Comunicaciones en Oficinas Centrales.	$12.522.032	N/A

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. • Incorporación de nubes públicas.	$23,320,067	$33,397,652
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**	**$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."

I.IV 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.

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 al 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).

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".

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.

I.IV SOBRE EL OFICIO DE ADVERTENCIA AD-AATIC-078-2022 DEL 13 DE JULIO DE 2022.

Mediante el oficio de advertencia indicado, esta Auditoría comunicó al Dr. Roberto Cervantes Barrantes, gerente general y a la Máster Idannia Mata Serrano, subgerente a.i de la Dirección de Tecnologías de Información y Comunicaciones la urgente necesidad de disponer de un sitio alterno de procesamiento de datos que eventualmente permitiría la continuidad y disminuiría el nivel de impacto por la suspensión de los servicios materializados tanto por el ataque cibernético conocido.

Además, entre otros aspecto se señaló la importancia de disponer de este elemento en la infraestructura tecnológica con la finalidad de continuar prestando los servicios ante eventuales interrupciones por la materialización de diversos riesgos humanos (huelgas, sabotajes, ciberataques, incendios), naturales (inundaciones, rayos, terremotos) o tecnológicos (carencia de fluido eléctricos, daño de quipos, afectaciones en telecomunicaciones), aportando un factor que permita responder a estas eventualidades en menor tiempo disminuyendo la afectación a los usuarios.

Adicionalmente, el Ing. Roberto Blanco Topping, subgerente a.i, en ese momento, comunicó[3] a esta Auditoría, que la DTIC no dispone de un centro de procesamiento de datos alterno o secundario, donde en caso de materializarse un riesgo inhabilitando el acceso a los servicios del sitio principal pueda dar continuidad a las operaciones habituales, además indicó al respecto de este tema que la habilitación del sitio alterno no garantiza en todos los casos la recuperación de los servicios al necesitar que las plataformas se encuentren interconectadas para poder mantener actualizado en tiempo real los datos y propiciar la disponibilidad y la habilitación y configuración de los accesos a ambos puntos.

Finalmente, en el apartado consideraciones este Órgano de Control indicó que dado el nivel de automatización de los servicios reflejado en un mayor desarrollo de sistemas, así como en un constante crecimiento del volumen de información en todos los ámbitos en los cuales se desempeña la institución y de la materialización del riesgo como resultado del ciberataque sufrido el 31 de mayo de 2022, cuyo efecto más relevante fue la suspensión de la operación de los servicios de tecnologías de información y comunicaciones, resulta de vital importancia concretar los esfuerzos iniciados a efectos de dotar a la institución de un sitio alterno de procesamiento de datos asegurando al menos el funcionamiento mínimo de aquellos elementos que se consideren de carácter crítico ante una interrupción.

Aunado a lo anterior, se requiere la definición del modelo y el alcance de esta herramienta, así como de los protocolos para su entrada en funcionamiento, dentro de las estrategias de manejo de crisis que disponga la institución, considerando la revisión de los antecedentes y estado actual del proyecto para su adquisición, cumpliendo con la normativa técnica y administrativa correspondiente contando con la participación oportuna de los entes asesores y de dirección institucionales en esta materia.

II. ESTADO DE SITUACIÓN DEL SITIO ALTERNO DE PROCESAMIENTO DE DATOS DE LA GERENCIA DE PENSIONES.

Con la finalidad de verificar el estado de situación relacionada con la operación del sitio alterno de procesamiento de datos de la Gerencia de Pensiones, se procedió a solicitar información al Licenciado Marco Gonzalez Jiménez jefe a.i del Centro de Gestión Informática de la Gerencia de Pensiones, mediante una sesión de trabajo por la plataforma institucional TEAMS el 8 de agosto de 2022, cuyos resultados fueron comunicados por el Lic. González Jiménez mediante el oficio GP-AGI-0262-2022, en lo que interesa indicó:

> *"(…) debo indicarle que en la Gerencia de Pensiones se tiene un esquema de sitio principal ubicado en el edificio Jorge Debravo y un sitio alterno en CODISA esto para las bases de datos de los sistemas CORE que se administran en esta gerencia a saber:*
>
> - *Sistema Integrado de Pensiones.*
> - *Sistema de Gestión de Créditos.*
> - *Sistema de Gestión de Inversiones.*

[3] Oficio GG-DTIC-2633-2022, del 23 de mayo de 2022.

Antes de que la CCSS sufriera el ataque, nuestro esquema de replicación estaba en línea a través de una solución de Microsoft SQL Server denominada Always On availability groups, que permiten una recuperación ante desastres casi inmediata. A través de esta replica también disponemos de un nodo de consulta en el sitio alterno que nos permite el balanceo de cargas con el ambiente productivo, ya que utilizamos este nodo para direccionar las consultas que se generan producto de la integración con aplicativos como validación de derechos, App EDUS y CCSS móvil.

Después del ataque y ante la necesidad de restablecer servicios en modo de contingencia en la Gerencia de Pensiones el esquema de replicación tuvo que eliminarse debido a que el nodo de CODISA no se encontraba disponible y no teníamos acceso para revisar su estado. Esta situación provoco que una vez que los compañeros de la DTIC nos dieron acceso al nodo de CODIDA (sic) este levantara con muchos errores por la forma en cómo se deshabilito la replicación*.*

En una sesión de trabajo que se tuvo con personal experto de Microsoft, en la que se trató de restablecer el servicio de replicación, se determinó que las condiciones actuales de los nodos presentaban muchos errores que no permitían levantar los servicios y aunque se trató de replicar la configuración en los nuevos DNS y Controladores de Dominio con la intervención de los compañeros de la DTIC no fue posible corregir el problema.

Hoy tenemos varios escenarios que queremos probar para intentar recuperar la replicación en línea, pero para poder llevarlo a cabo se requiere la disponibilidad de los compañeros que administran el AD y los DNS, esto debido a que ante la situación actual de la institución estos servicios están centralizados y ya no tenemos acceso, razón por la cual no ha sido fácil tener acceso a estos recursos ya que la demanda es muy alta y los recursos muy escasos.

Seguiremos insistiendo hasta lograr restablecer el servicio de replicación en línea con nuestro sitio alterno ya que para nosotros en la Gerencia de Pensiones es de suma importancia contar con este servicio lo antes posible*." (lo resaltado no corresponde al original)."*

III. CONSIDERACIONES NORMATIVAS

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)."*

Al respecto el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, establece como un objetivo de esa unidad:

> *"Garantizar la continuidad de la gestión de Tecnologías de Información y Comunicaciones en situaciones de emergencia o desastres, mediante la administración e implementación de procesos alternos de trabajo, planes de contingencia, de recuperación de la información y capacidad operativa.".*

Asimismo, el citado manual define como una activad sustantiva de la subárea de seguridad y calidad informática, verificar por la continuidad de la gestión.

El Modelo de Organización de Centros de Gestión Informática, en su apartado 5.5.19 Política de Atención de Emergencias y Desastres, señala:

> *"Las diversas unidades de trabajo bene elaborar planes de emergencias, para prevenir, mitigar, atender los eventos que se puedan presentar, salvaguardar la vida, las inversiones y la continuidad de los servicios.".*

Adicionalmente, respecto a la gestión técnica de los Centros de Gestión Informática de nivel gerencial, indica:

> *"Implementar Planes de Contingencia y Recuperación de Tecnologías de Información, en su ámbito de competencia, de acuerdo con la normativa vigente interna y externa, con el objetivo de mantener la continuidad de los servicios.".*

IV. CONSIDERACIONES FINALES

En virtud de lo anterior y en concordancia con lo advertido por esta Auditoría en el oficio AD-ATIC-078-2022 del 13 de julio de 2022 es vital disponer de un sitio alterno de procesamiento de datos funcional como parte de la infraestructura tecnológica, tanto de los servicios brindados por el seguro de salud como aquellos que corresponden al régimen de invalidez vejez y muerte (pensiones), que minimicen los riesgos asociados a interrupciones al detectarse una afectación en el sitio principal, como ocurrió el 31 de mayo de 2022, así como de la materialización de futuros eventos, lo anterior con el fin de garantizar la continuidad en las operaciones cotidianas.

Ciertamente, según lo indicado por el Lic. Marco Gonzalez Jiménez, jefe a.i del Centro de Gestión Informática, la Gerencia de Pensiones dispone de un esquema de sitio principal ubicado en el edificio Jorge Debravo, sede de esa unidad y alterno en CODISA (sitio de procesamiento principal institucional), que aloja las bases de datos de los sistemas integrado de pensiones, gestión de créditos y sistema de inversiones, además de utilizarse para la gestión de las consultas que se efectúan a dichas bases de datos.

En ese contexto, fueron suspendidos los servicios de replicación de datos y consultas dirigidas a los servidores en esa ubicación, además de las derivadas en la integración de aplicaciones como validación de derechos en línea, app EDUS y CCSS móvil, entre otros, que permitían balancear la cantidad de transacciones a ejecutar en los servidores principales. Aunado a lo anterior, la suspensión abrupta de los servicios ocasionó dificultades en la recuperación posterior debido a errores en la configuración de los DNS[4] y Controladores de Dominio[5].

En ese orden de ideas, en vista de la afectación en el acceso a las bases de datos de la Gerencia de Pensiones ubicadas en el sitio principal institucional (CODISA), resulta relevante, en su rol de gestor de la información, infraestructura y servicios tecnológicos necesarios para la prestación de sus servicios así como para asegurar la continuidad del negocio, ejecute las acciones necesarias con la finalidad de determinar con la asesoría y participación de la Dirección de Tecnologías de Información y Comunicaciones en su rol de rectoría en este materia si la actual arquitectura brindada en dicha gerencia respecto del procesamiento principal y alterno es pertinente tanto desde el punto de vista integral de la CCSS como específico para las unidades adscritas a la misma, de forma tal que cumplan las condiciones requeridas en cuanto a eficiencia, eficacia, disponibilidad y demás elementos necesarios para garantizar la operacionalidad de los sistemas.

Lo anterior valorando tanto el modelo y alcance de la solución implementada, como adicionalmente revisando las diversas alternativas de solución en esta materia y efectuando los ajustes y mejoras correspondientes, en consonancia con el marco normativo y las mejores prácticas tecnológicas, de gobierno y económicas.

[4] El DNS, o sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas (por ejemplo, 192.0.2.44).
[5] Un controlador de dominio (DC) es un servidor que responde a las solicitudes de autenticación de seguridad dentro de un dominio de Windows Server. Es un servidor en una red de Microsoft Windows o Windows NT que es responsable de permitir el acceso del host a los recursos del dominio de Windows. Un controlador de dominio es la pieza central del servicio de Active Directory de Windows. Autentica a los usuarios, almacena la información de la cuenta del usuario y aplica la política de seguridad para un dominio de Windows.

En virtud de lo expuesto, se brinda a esa Administración la presente asesoría con el propósito de que se adopten las medidas pertinentes, a fin de ejecutar las acciones que correspondan, en aras de valorar la arquitectura de procesamiento de datos principal y alterno implementada por la Gerencia de Pensiones y ejecutar las acciones que permitan fortalecerla considerando la inclusión de elementos críticos para asegurar la continuidad de los servicios tecnológicos que soportan las prestaciones brindadas por esa gerencia.

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, así como por otros riesgos ya identificados o eventos de carácter imprevisto que se presenten en el futuro.

En virtud de lo expuesto, y con el fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se da conocer la información descrita, con el propósito de ser sometida a valoración y revisión por esa Administración, de forma tal que se fortalezcan los procesos relacionados con la prestación continua de los servicios mediante la valoración de las oportunidades de mejora del modelo de sitio alterno de procesamiento de datos implementado actualmente por esa gerencia, considerando el criterio del ente rector, a efectos de minimizar la exposición al riesgo materializado durante el ciberataque, así como de otros eventos que puedan presentarse posteriormente.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.10.05 14:01:10 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/AAM/lbc

C. Máster Marta Eugenia Esquivel Rodríguez presidenta, Presidencia Ejecutiva -1102.
Doctor Roberto Cervantes Barrantes, gerente, Gerencia General – 1100.
Máster Idannia Mata Serrano, subgerente a.i, Dirección de Tecnologías de Información y Comunicaciones – 1105.
Auditoría.