ATIC-166-2020
11 de diciembre de 2020

RESUMEN EJECUTIVO

El presente estudio se realizó de conformidad con el Plan Anual Operativo 2020 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de analizar la gestión integral de la Plataforma Tecnológica Central a cargo de la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

Los resultados del estudio permitieron evidenciar que la Caja Costarricense de Seguro Social no dispone de una estrategia integral de gestión de la Plataforma Tecnológica Central, que le permita no solo la continuidad y calidad de sus prestaciones, sino también se efectúe un mejor aprovechamiento de los recursos institucionales, con un enfoque de sostenibilidad y disponibilidad que apoyen las decisiones sobre la ruta tecnológica establecida, mediante los estudios pertinentes que debe realizar.

Lo anterior, considerando las inversiones que ha realizado la Institución en los últimos seis años por más de 15 millones de dólares, así como la dependencia para su funcionamiento, de las unidades de negocio tanto de misión crítica como de apoyo administrativo, de esa infraestructura,

Adicionalmente, aun no hay definición sobre el sitio que funcionaría como Centro de Datos Principal y Sitio Alterno, lo anterior a pesar de que actualmente la Dirección de Tecnologías de Información presentó ocho alternativas para revisión y aprobación al 30 de noviembre de 2020.

Así mismo, se determinaron oportunidades de mejora en torno a establecimiento de un Plan de Capacidad de los equipos de la Plataforma Tecnológica Central, el cual contribuya a la identificación de requerimientos y a la planificación integral de la infraestructura que soporta la operación de las diferentes soluciones de negocios de la Institución.

Por otra parte, se identificó la ausencia de pruebas integrales o simulacros para verificar la continuidad de los servicios brindados por la Plataforma de marras con la participación de los dueños de los procesos y la Dirección de Tecnologías de Información y Comunicaciones. Aunado a lo anterior, se detectaron aspectos de mejora vinculados con la actualización del documento denominado Plan de Continuidad para la Gestión del Área de Soporte Técnico y el registro correspondiente de las firmas de los responsables.

Adicionalmente, se constató la falta de un Plan de Remplazo de los activos que constituyen la plataforma supra citada, en el cual se identifiquen las necesidades de adquisición de hardware y software de manera integral, así como la proyección de inversiones periódicas, lo cual reviste importancia por cuanto se detectaron 49 de 233 componentes tecnológicos de esa plataforma, totalmente depreciados y 106 con una vida útil inferior al 50%.

Respecto a la rendición de cuentas sobre la gestión de la Plataforma Tecnológica Central mediante informes mensuales, no se obtuvo el respaldo documental asociado a la validación de indicadores que permita la toma de decisiones por parte de la Dirección de Tecnologías de Información y Comunicaciones, así como el proceso de retroalimentación con el Área de Soporte Técnico y sus unidades a cargo.

También, se visualizó la definición de las métricas para efectuar las actividades de monitoreo mediante correos electrónicos remitidos por diversos funcionarios, sin que se confeccionara y oficializara la documentación formal con las validaciones y aprobaciones del nivel superior jerárquico.

Finalmente, resulta oportuno la Administración efectúe la gestión de riesgos asociados a la adquisición de servicios de terceros para el albergue del Centro de Datos Principal, la eventual dependencia de proveedores de servicios considerando el tiempo en el cual la institución ha contratado este tipo de actividades con la empresa Ideas Gloris S.A., así como el plazo de tiempo disponible entre el desarrollo del nuevo proceso contractual y la vigencia de la última prórroga del Contrato N°001-2017.

En virtud de lo expuesto, este Órgano de Fiscalización emitió conclusiones y recomendaciones con la finalidad de que la Dirección de Tecnologías de Información y Comunicaciones fortalezca el sistema de control interno para que disponga de una estrategia integral para la gestión de la PTC que oriente la planificación, ejecución, seguimiento y valoración de las diversas actividades sustantivas a su cargo vinculadas con la Plataforma Tecnológica Central, actualizaciones del Plan de Continuidad de los servicios TIC y del negocio con sus respectivos simulacros, la planificación de la capacidad y el remplazo de los componentes de la Plataforma mencionada anteriormente, la formalización de las métricas vinculadas con su monitoreo, validaciones del cumplimiento de los procesos con base en los indicadores establecidos, así como la valoración de riesgos respecto a la solución de hospedaje del Centro de Datos Principal.

ATIC-166-2020
11 de diciembre de 2020

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES
AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN INTEGRAL DE LA PLATAFORMA TECNOLÓGICA CENTRAL

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES UE- 1150

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo 2020 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión integral de la Plataforma Tecnológica Central que soporta las soluciones informáticas de la Caja Costarricense del Seguro Social.

OBJETIVOS ESPECÍFICOS

1. Verificar la gestión del proyecto ejecutado por la Dirección de Tecnologías de Información y Comunicaciones denominado “Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central”.
2. Revisar la definición de los sitios principal y alterno del centro de datos adoptados por la Institución.
3. Analizar los indicadores establecidos para la gestión de la Plataforma Tecnológica Central, así como la planificación de la capacidad.
4. Identificar las soluciones de contingencia diseñadas para brindarle continuidad a los servicios brindados por la Caja Costarricense del Seguro Social a través de la Plataforma Tecnológica Central.
5. Analizar el Plan de Remplazo de los activos que conforman la Plataforma Tecnológica, así como las inversiones efectuadas para su mantenimiento y fortalecimiento.

ALCANCE

El estudio comprende las acciones realizadas por la Dirección de Tecnologías de Información y Comunicaciones, en torno a la gestión integral de la Plataforma Tecnológica Central de la CCSS. Lo anterior, considerando el periodo comprendido entre enero 2017 y octubre 2020.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Revisión del respaldo documental suministrado por la Administración Activa respecto a la gestión de la Plataforma Tecnológica Central (inversiones efectuadas, presupuesto asignado, contrataciones, informes de rendición de cuentas, Plan de Capacidad, normativa, entre otros).

- Aplicación de entrevistas y consultas a los siguientes funcionarios:

- Máster Robert Picado Mora, Subgerente de la Dirección Tecnologías de Información y Comunicaciones.
- Máster Christian Chacón Rodríguez, Subdirector de Tecnologías de Información y Comunicaciones.
- Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico
- Máster Alexander Ordoñez Arroyo, Jefe de la Subárea de Administración de la Plataforma Tecnológica Central
- Máster Mario Vilchez, Jefe de la Subárea de Aseguramiento de la Calidad a/c del Área de Calidad y Seguridad
- Lic. Geiner Gamboa Otárola, Jefe de la Subárea de Gestión de la Producción.
- Máster Adriana Moreira Madrigal, encargada del proyecto de Contratación 2019LA-000012-1150 *"Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk Management".*
- Máster Róger Palavicini Villalobos, colaborador del proyecto de Contratación 2019LA-000012-1150 *"Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk Management"*.

MARCO NORMATIVO

- Constitución Política de la República de Costa Rica, 2015.
- Ley General de Control Interno, No. 8292.
- Reglamente a la Ley de Contratación Administrativa, 2018.
- Normas de Control Interno para el Sector Público, 2009.
- Normas Técnicas para la Gestión y Control de las Tecnologías de la Información (CGR), 2007.
- Normas Institucionales en TIC, 2012.
- Políticas de Seguridad Informática Institucionales, 2007.
- Lineamientos Generales de Inventario TIC TIC–INV-0001, 2011.
- Lineamientos para la definición de planes de capacidad en la Plataforma Tecnológica Central de Tecnologías de Información y Comunicaciones, 2015.
- Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, ASCI-UCG-ORG-002, 2013.
- Guía Evaluación del reemplazo de activos de TIC DTI-I-IN-0002, 2012.
- Esquema de la Continuidad de los Servicios Informáticos del Área de Soporte Técnico DTI-IST-0001, 2018.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)"*

ANTECEDENTES

El concepto de Plataforma Tecnológica se refiere al entorno informático constituido por el conjunto de software y hardware donde se gestionan y ponen en operación los aplicativos y soluciones de negocios compatibles entre sí. Al respecto, la Institución dispone del documento *"Modelo de Infraestructura Tecnológica TIC-MIT-0001"* de la Dirección de Tecnologías de Información y Comunicaciones, en el cual se indica como objetivo de éste el brindar

un ambiente de trabajo seguro, confiable e íntegro, propiciando con ello la continuidad y disponibilidad de la información.

Otro concepto importante es el de centro de procesamiento de datos, el cual es el lugar donde se concentran todos los recursos necesarios para la gestión de la información de una organización. Normalmente se trata de un edificio o sala de gran tamaño, con las adecuadas condiciones físicas y lógicas, usado para mantener en él una gran cantidad de equipamiento electrónico que alberga soluciones.

Sobre este tema, la Caja Costarricense del Seguro Social, mediante la Licitación Nacional N° 2017LN-000001-1150, *"Servicio de Hospedaje para Albergar el Centro de Cómputo Principal de la CCSS",* contrató los servicios de hospedaje del Centro de Cómputo Principal, cuya adjudicación se realizó el 5 de junio de 2017 a la empresa Ideas Gloris S.A. por un monto total de $600.000.00 (Seiscientos mil dólares exactos) y con una vigencia de 12 meses a partir del 18 de agosto de 2017. Además. se definió en el contrato No. 002-2017 la posibilidad de realizar prórrogas por hasta 3 periodos adicionales.

Actualmente, el Centro de Cómputo Principal (CCP) institucional se ubica en el Parque Tecnológico CODISA[1] en Tibás y su administración está a cargo de la Dirección de Tecnologías de Información y Comunicaciones, específicamente del Área de Soporte Técnico. En dicha Plataforma se almacenan los principales sistemas de información y las bases de datos institucionales utilizados en la prestación de servicios a los asegurados, patronos, pensionados, entre otros.

Dentro de los aplicativos y repositorios de datos resguardados en los componentes que conforman la Plataforma Tecnológica Central se encuentran el Sistema Centralizado de Recaudación (SICERE), Expediente Digital Único en Salud (EDUS), Sistema de Presupuesto Institucional (SIP), Sistema de Registro y Control de Pago de Incapacidades (RCPI), Sistema de Gestión de Suministros (SIGES), Sistema Control de Bienes Muebles (SCBM), Sistema Integrado de Comprobantes (SICO) y Módulo Integrado de Seguridad (MISE).

Aunado a esto, se brindan servicios tecnológicos como el de internet, intranet, correo electrónico, antivirus y el Active Directory[2].

Inversiones relacionadas con la Plataforma Tecnológica Central

Al respecto, en la siguiente tabla se presentan el monto de las inversiones efectuadas a la Plataforma Tecnológica Central relacionadas con contrataciones, agrupadas por año:

Tabla No.1
Inversiones efectuadas en torno a la Plataforma Tecnológica Central
2014-2020

Año	Monto de la inversión (Contrataciones)
2014	$5 627 475,84
2015	$387 400,00
2016	$0
2017	$3 626 980,31
2018	$2 114 790,56
2019	$2 865 249,61
2020	$1 239 737,93
Total	**$15 861 634,25**

Fuente: Información suministrada por la Dirección de Tecnologías de Información y Comunicaciones.

[1] Empresa costarricense que ofrece productos y servicios de tecnologías de información para los sectores: financiero, gobierno y privado. Ofrece soluciones de Centro de Datos, Almacenamiento en la Nube, Software, entre otros.
[2] Un directorio es una estructura jerárquica que almacena información sobre objetos en la red. Un servicio de directorio, como Active Directory Domain Services (AD DS), proporciona los métodos para almacenar datos de directorio y hacer que estos datos estén disponibles para los usuarios y administradores de la red.

Como se visualiza en la tabla No. 1, en los años 2014 y 2017 fueron los periodos en los cuales se invirtieron los montos más significativos mediante la gestión de contrataciones para el fortalecimiento de la Plataforma Tecnológica con montos de $5 627 475,84 (cinco millones seiscientos veintisiete mil cuatrocientos setenta y cinco dólares con 84/100) y $3 626 980,31 (tres millones seiscientos veintiséis mil novecientos ochenta dólares con 31/100), posteriormente, en el 2019 se efectuó una erogación monetaria de $2 865 249,61 (dos millones ochocientos sesenta y cinco mil doscientos cuarenta y nueve dólares con 61/100), en el 2018 se ejecutaron $2 114 790,56 (dos millones ciento catorce mil setecientos noventa dólares con 56/100), en el 2020 $1 239 737,93 (un millón doscientos treinta y nueve mil setecientos treinta y siete dólares con 93/100) y finalmente en el 2016 no se efectuaron inversiones relacionadas con esta temática.

Según el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central, gestionado por la Dirección de Tecnologías de Información y Comunicaciones, para el desarrollo de las etapas conceptualizadas en el Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central (Centro de Datos), se han ejecutado una serie de proyectos para el reforzamiento de la infraestructura actual.

A continuación, el detalle de contrataciones efectuadas por la Dirección de Tecnologías de Información y Comunicaciones durante el periodo 2013 al 2020 relacionadas con Plataforma Tecnológica Central.

Tabla No. 2
Contrataciones efectuadas por la DTIC en relación con la Plataforma Tecnológica Central
Periodo 2013-2020

Número	Contrato / Orden de compra	Objeto	Monto total contratación
2015LN-000012-05101	2016-000008-00	Contratación del Reforzamiento de la Plataforma Tecnológica Institucional	$ 1,455,079.78
2015LA-000008-1150	008-2015	Renovación de Licenciamiento y Servicios de Ingeniería para la Plataforma Citrix	$ 387,400.00
2015LN-000012-05101	2017-000012	Aplicación articulo 209 Contratación del Reforzamiento de la Plataforma Tecnológica Institucional	$ 674,957.20
2017LA-000001-1150	006-2017	Adquisición de un Clúster de dos equipos balanceadores de cargas basadas en IP, Licenciamiento y Mantenimiento	$ 317,598.00
2017LA-000010-1150	036-2017 037-2017	Accesorios para equipos de comunicación CISCO, Blades Lenovo, y Sistema de almacenamiento Storwize V7000	$ 416,740.84
2017LN-000002-1150	001-2018	Solución de alta disponibilidad para soportar Sistema Centralizado de Recaudación SICERE y APEX, BDADMIN, MDI, MISE, PORTALRH, SCBM, SICS, SIGC, SIGES	$ 1,169,013.07
2013LN-00001-1150	004-2014	Servicios de monitoreo de la plataforma tecnológica institucional, Ítem N° 03 (tercera prorroga)	$ 936,000.00
2013LN-00001-1150	003-2014	Servicios de soporte, ingeniería y mantenimiento de la plataforma tecnológica institucional, Ítem N° 01 y 02 (tercera prorroga)	$ 4,691,475.84
2017CD-000007-1150	011-2017	Servicios de Mantenimiento Correctivo para plataforma de servidores Blade HP"	$ 40,782.00
2017CD-000007-1150	011-2017	artículo 208 del RLCA, Adenda la orden de compra 011-2017, 2017CD-000007-1150, "Servicios de mantenimiento correctivo para plataforma de servidores Blade HP"	$ 20,391.00
2017LA-000008-1150	011-2017	Adquisición de una solución Hardware y Software para respaldos a Disco	$ 721,822.49
2017LA-000028-1150	042-2017	Adquisición de un sistema de almacenamiento para recuperación de desastres para el EDUS	$ 113,107.46
2013LN-00001-1150	004-2014	Ampliación por 6 meses, Licitación N°2013LN-00001-1150, OC. 034-2014. Servicios de monitoreo de la plataforma tecnológica institucional, Ítem N° 03 (art 208)	$ 117,000.00
2017LN-000002-1150	015-2018	Ampliación 50% Solución de alta disponibilidad para soportar Sistema Centralizado de Recaudación SICERE y APEX, BDADMIN, MDI, MISE, PORTALRH, SCBM, SICS, SIGC, SIGES	$ 581,802.19
2018LA-000003-1150	002-2018	Servicios de Mantenimiento para la Plataforma Tecnológica Central HP	$ 300,827.24
2018LN-000016-1150	001-2019	Solución de reemplazo de los SAN Switch CORE del DataCenter y reemplazo de cableado FC	$ 877,882.41

Número	Contrato / Orden de compra	Objeto	Monto total contratación
2018LA-000014-1150	038-2018 039-2018	Accesorios para plataforma tecnológica	$ 159,817.93
2018CD-000022-1150	037-2018	Accesorios para Tecnológicas de Almacenamiento IBM	$ 460,238.97
2018LA-000015-1150	043-2018	"Componentes para plataforma tecnológica LENOVO	$ 287,610.22
2018CD-000008-1150	020-2018	Servidores RISC para servicios de recaudación del SICERE	$ 73,995.55
2019LA-000005-1150	008-2019	Chasis (enclousure) con unidades de procesamiento tipo Blade	$ 288,537.00
2019LA-000012-1150	019-2019	Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk Management	$ 510,850.00
2019LA-000020-1150	038-2019	Solución para el reemplazo de los SAN Switches CORE del Datacenter Piso 11 Edificio Jenaro Valverde	$ 217,155.22
2019LA-000017-1150	034-2019 035-2019	Accesorios Varios para la Plataforma Tecnológica	$ 529,817.13
2019LA-000017-1150		Aplicación articulo 209 RLCA al contrato No.034-2019 de la Licitación Abreviada No.2019LA-000017-1150.	$ 159,968.89
2019LA-000019-1150	002-2020	Solución de Almacenamiento y Gestión de Datos NO Estructurados	$ 287,301.82
2020CD-000007-1150		Actualización y soporte balanceadores F5	$ 64,462.00
TOTAL			**$15,861,634.25**

Fuente: Información suministrada por la Dirección de Tecnologías de Información y Comunicaciones mediante oficio GG-DTIC-3967-2020.

Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central (Centro de Datos)

De acuerdo con el Plan de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central, emitido por la Dirección de Tecnologías de Información y Comunicaciones, el objetivo de esta iniciativa es asegurar la operación continua de la Plataforma Tecnológica de la CCSS, para garantizar la disponibilidad, confiabilidad y seguridad de la información de los sistemas institucionales críticos, a partir del desarrollo de los entornos lógico, físico, geográfico y tecnológico necesarios.

Se plantearon dos etapas, la primera hace referencia a la necesidad de reforzar la plataforma tecnológica, aumentando la capacidad, memoria, procesamiento y almacenamiento de los equipos y la segunda contempló la realización del Estudio de Factibilidad o Preinversion para determinar la opción para habilitar el nuevo centro de datos.

El 13 de noviembre de 2014, mediante sesión N°8751, la Junta Directiva de la Caja Costarricense de Seguro Social, en el artículo 10° se 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 contar con un Centro de Datos Principal y un Centro de Datos Alterno.

De acuerdo con lo expuesto, el Máximo Jerarca Institucional acordó en el artículo 18° de la sesión N°8768, 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 de avance del proyecto en cuestión.

En ese mismo orden de ideas, el Proyecto fue presentado en la sesión N°8831 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 la presentación de avances alcanzados.

El Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, mediante oficio GG-DTIC-6363-2020 del 23 de octubre de 2020, le remitió al Doctor Roberto Cervantes Barrantes, Gerente General, el documento denominado *"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 señalaron las acciones ejecutadas para el desarrollo tecnológico de la Caja Costarricense del Seguro Social, así como la inclusión del análisis de las siguientes ocho alternativas:

Tabla No.3
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. • Operación de equipos por leasing a demanda. • 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. • Adquisición de equipamiento tecnológico. • 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. • 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. • 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.

El documento mencionado anteriormente incluyó el dictamen financiero sobre los costos en los cuales incurriría la institución ante el desarrollo e implementación de cada una de las alternativas propuestas. En la siguiente tabla se presentan los resultados del estudio de mercado realizado:

Tabla No.4
Resultados del Estudio de Mercado relacionado con las alternativas propuestas

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.

Acuerdos de Junta Directiva asociados al Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central

Los últimos tres acuerdos emitidos por el máximo Órgano Colegiado relacionados con el proyecto mencionado se describen a continuación.

Artículo N°13, Sesión N°9004 del 3 de diciembre de 2018:

"ARTICULO 13°

Se tiene a la vista el oficio N° GIT-8394-2017, del 16 de agosto de 2017, que firma la señora Gerente de Infraestructura y Tecnologías y presenta el informe estado de avance Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos) para la toma de decisión. (Art. 18° Sesión N° 8768) Se complementa con la nota en CD GIT-8394-2017 y oficio DTIC-4867-2017.

Con base en lo expuesto, considerando el informe DTIC-4867-2017 y documentos anexos, mediante el cual el Ing. Robert Picado Mora, Subgerente Dirección de Tecnologías de Información y Comunicaciones, presenta el informe sobre estado del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica, para conocimiento y toma de decisión de la Junta Directiva ACUERDA:

ACUERDO PRIMERO: dar por recibido los Informes de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), que atienden lo instruido en el artículo 18 de la Sesión 8768.

ACUERDO SEGUNDO: dar por conocida la estrategia definida por la Dirección de Tecnologías de Información y Comunicaciones, para que la Caja Costarricense de Seguro Social disponga de un Centro de Procesamiento Principal y un Centro de Procesamiento Alterno para garantizar la prestación de los servicios tecnológicos tanto a lo interno como externo de la Institución.

ACUERDO TERCERO: instruir a la Gerencia de Infraestructura y Tecnologías, la presentación de un informe en tres meses sobre el avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional.
ACUERDO FIRME."

Artículo N°16, Sesión N°9035 del 30 de abril de 2019:

"ARTICULO 16°:

Por consiguiente, conocidos los términos del oficio número GG-0417-2019, de fecha 30 de abril de 2019, que firma el doctor Cervantes Barrantes, Gerente General y que en adelante se transcribe en lo pertinente, y que contiene el informe de avance del Proyecto de Fortalecimiento de la arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos):

"En el acuerdo tercero de la sesión 9004 en su artículo 13, la Junta Directiva solicitó lo siguiente:

"ACUERDO TERCERO: instruir a la Gerencia de Infraestructura y Tecnologías, la presentación de un informe en tres meses sobre el avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional."

Se remite el informe por parte de la Gerencia General, dado que en el acuerdo segundo del artículo 4° en la sesión 9024 se dispuso lo siguiente:

"ACUERDO SEGUNDO: se trasladan las direcciones de Tecnologías de Información y Comunicación (TIC), Comunicación Organizacional, Administración y Gestión de Personal, y CENDEISSS a depender de la Gerencia General, a partir de que quede en firme la propuesta." y habiéndose hecho la presentación por parte del ingeniero Christian Chacón Rodríguez, subdirector de la Dirección de Tecnologías de Información y Comunicación, la Junta Directiva ACUERDA:

ACUERDO PRIMERO: dar por recibido el Informe de Avance del Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos), que atiende lo instruido en el artículo 13 de la Sesión 9004 del 3 de diciembre del 2018.

ACUERDO SEGUNDO: instruir a la Dirección de Tecnologías de Información y Comunicaciones, establecer un lapso, para que el señor Presidente Ejecutivo de la CCSS pueda reunirse con la Presidencia Ejecutiva y autoridades del ICE, para explorar una mejor alternativa económica.
ACUERDO FIRME""

Artículo N°27, Sesión N°9039, del 27 de junio de 2019:

"ARTICULO 27°

De acuerdo con lo deliberado y con base en el informe verbal del Dr. Román Macaya Hayes, Presidente Ejecutivo, sobre la reunión sostenida con la Presidenta Ejecutiva del ICE, la Junta Directiva ACUERDA:

ACUERDO PRIMERO: dar por atendido el artículo 16° de la sesión N° 9035.

ACUERDO SEGUNDO: Instruir a la Gerencia General y a la Dirección de Tecnologías de Información para que continúen las gestiones necesarias con el ICE sobre la temática del Data Center.
ACUERDO FIRME"

Modelo de Gobernanza de TIC y Plataforma Tecnológica Central.

A continuación, se describen las iniciativas correspondientes de ejecución a corto, mediano y largo plazo dentro de la transición e implementación del Modelo meta de Gobernanza de las TIC y la Seguridad de la Información, las cuales tienen relación con la Plataforma Tecnológica Central:

Tabla No.5
Iniciativas del Modelo de Gobernanza asociadas a la Plataforma Tecnológica Central

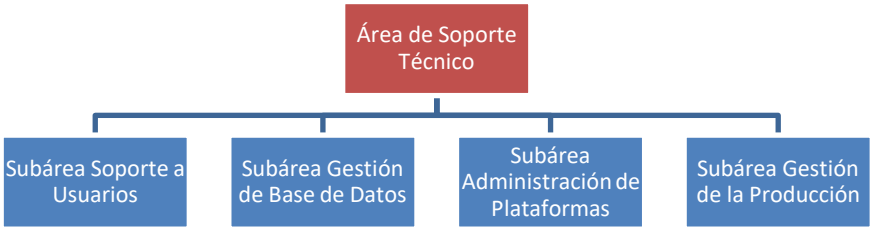
Iniciativa	Plazo de ejecución
Habilitar la gestión de eventos de la plataforma tecnológica central y los servicios TIC	Corto plazo
Habilitar la gestión de las operaciones de TIC	Corto plazo
Implementar la Gestión de la Arquitectura de Empresarial	Mediano plazo
Consolidar el centro procesamiento principal y el centro de procesamiento alterno de la CCSS	Mediano plazo
Habilitar la gestión de activos y configuración	Mediano plazo
Habilitar la gestión de la continuidad de negocio	Mediano plazo
Habilitar la gestión financiera de TIC	Largo Plazo
Adaptar la gestión de proveedores	Largo Plazo

Fuente: Elaboración propia basada en documentación del Proyecto Modelo Meta de Gobernanza de las TIC y Seguridad de la Información.

Estructura Organizacional de la Dirección de Tecnologías de Información y Comunicaciones en relación con la gestión de la Plataforma Tecnológica Central

En agosto de 2013, mediante el articulo N°32 de la Sesión N°8658, la Junta Directiva aprobó la versión vigente el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, estableciendo entre otros aspectos las unidades que la componen y sus actividades sustantivas. Así mismo, en lo que respecta específicamente a la gestión de Plataforma Tecnológica Institucional, se definió al Área de Soporte Técnico como el responsable de su modernización y mantenimiento, para lo cual se estableció el siguiente esquema estructural:

Figura No.1
Estructura Organizacional del Área de Soporte Técnico



Fuente: Elaboración propia basada en el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, 2013.

Aunado a lo anterior, para el cumplimiento de las responsabilidades definidas para el Área de Soporte Técnico y las subáreas se detallaron las siguientes actividades sustantivas:

Área de Soporte Técnico

- Optimizar el uso de los recursos tecnológicos, con base en las posibilidades técnicas y los indicadores definidos, con la finalidad de lograr en el corto plazo el retorno de la inversión en tecnologías de información.
- Gestionar la adquisición de hardware y software requeridos en su ámbito de competencia, con base en las necesidades de la organización y las políticas y estrategias vigentes, con el objeto de modernizar el desarrollo de la gestión.
- Controlar el desarrollo de la plataforma tecnológica, con base en las políticas, la regulación establecida, el monitoreo y el uso de los recursos tecnológicos, con el propósito de agilizar la prestación de los servicios y la operación de los sistemas de información.
- Planificar la adquisición de las tecnologías de información y las comunicaciones en su ámbito de acción, a partir de los requerimientos institucionales y los nuevos avances en la materia, con el propósito de contar con las herramientas necesarias que permiten atender con oportunidad las demandas de los usuarios.

- Realizar el inventario de la plataforma tecnológica (hardware y software) en su ámbito de acción, con base en las políticas definidas, a efecto de contar con información que facilite la toma de decisiones y fortalezca los mecanismos de control.
- Gestionar la adquisición de las licencias requeridas para la plataforma tecnológica que se administra, de conformidad con los recursos disponibles y los requerimientos institucionales, con el objetivo de que los sistemas funcionen correctamente y contar con el respaldo de los proveedores.

Subárea de Gestión de la Producción

- Monitorear la plataforma tecnológica, con base en las tecnologías implementadas, con el propósito de reportar cualquier situación fuera de lo normal a las unidades y proveedores Involucrados en los contratos de mantenimiento.
- Administrar u otorgar el mantenimiento preventivo y correctivo de los equipos y dispositivos de la plataforma tecnológica, en atención a las políticas y los recursos disponibles, con la finalidad de que los equipos funcionen en forma efectiva.
- Elaborar los estudios técnicos y participar en la elaboración de los términos de referencia para la adquisición de la infraestructura necesaria para soportar la plataforma tecnológica, de acuerdo con los estándares definidos y los requerimientos institucionales, con el fin de contar con la plataforma idónea que permita el correcto funcionamiento de los sistemas informáticos.
- Planificar con las demás unidades relacionadas las necesidades de soporte de infraestructura, con base en los estándares y las prioridades institucionales, para optimizar los recursos disponibles.

Subárea Gestión de Usuarios

- Realizar el mantenimiento preventivo y correctivo del software de la plataforma computacional, con base en los planes elaborados, con el objetivo de que funcionen eficazmente y de optimizar los recursos institucionales.

Subárea de Administración de Plataformas

- Otorgar soporte técnico a los servidores de alta complejidad, con base en los requerimientos de los usuarios y la disponibilidad de recursos, con el propósito de lograr un óptimo aprovechamiento de la tecnología y el cumplimiento de los objetivos y metas de la organización.
- Depurar los sistemas operativos, a partir de los estándares definidos y recursos disponibles, para lograr efectividad en los tiempos de respuesta de la tecnología en sistemas de información.
- Promover la actualización tecnológica de los servidores institucionales, de acuerdo con los recursos financieros disponibles y las necesidades de la organización, con el fin de contar con herramientas actualizadas que garanticen la efectiva operación de los sistemas.
- Administrar el ambiente de servidores de alta complejidad, con base en las políticas y estándares definidos, con el propósito de lograr la operación eficaz de los mismos.
- Otorgar mantenimiento preventivo y correctivo a los sistemas operativos computacionales, de conformidad con los estándares y políticas definidas, a efecto de lograr la efectiva operación de los sistemas.
- Administrar el espacio en disco de los servidores de alta complejidad, con base en los requerimientos institucionales y los estándares definidos, con el propósito de garantizar la optimización de los recursos.
- Participar en la definición del hardware requerido para la administración de sistemas críticos, de acuerdo con las necesidades detectadas y la disponibilidad financiera, para la efectiva operación de los sistemas institucionales.
- Realizar pruebas de funcionamiento a los equipos de alta complejidad, a partir de las políticas, los estándares y los planes de trabajo establecidos, con el fin de detectar problemas y plantear las soluciones que correspondan.
- Participar en la elaboración de las especificaciones técnicas para la adquisición de servidores de alta complejidad, sistemas de almacenamiento, respaldo y demás componentes de la plataforma computacional, con base en los avances tecnológicos, los requerimientos institucionales y la normativa vigente, para contar con el equipo requerido que permita satisfacer en forma efectiva las necesidades de la organización.

- Realizar el mantenimiento preventivo y correctivo a los servidores de alta complejidad, con base en los recursos disponibles, los planes de trabajo establecidos y las necesidades de los usuarios, con el propósito de otorgar un servicio oportuno y de calidad.
- Otorgar el mantenimiento preventivo y correctivo a los sistemas de almacenamiento y respaldo, de acuerdo con las necesidades presentadas y los planes establecidos, con la finalidad de lograr su funcionamiento efectivo.
- Administrar el ambiente de Servidores, Sistemas Operativos, dispositivos de almacenamiento y el software de Servidores de Aplicaciones de alta complejidad, con base en los requerimientos, las políticas y los estándares definidos, con el propósito de garantizar la optimización de los recursos y la efectiva operación de los sistemas instituciones.
- Mantener la Plataforma Tecnológica actualizada, a partir de los requerimientos de los usuarios, las metodologías de trabajo e investigación realizada, con la finalidad de agilizar los servicios de procesamiento y almacenamiento vigentes en la Institución.
- Otorgar soporte técnico a los Servidores de Alta Complejidad, con base en los planes de trabajo establecidos, los requerimientos de los usuarios y la disponibilidad de recursos, con el fin de obtener un óptimo aprovechamiento de la tecnología y cumplir con las metas y objetivos de la Institución.
- Administrar la conectividad de las diversas aplicaciones, en respuesta a los requerimientos de los usuarios, los estándares y la ejecución de monitoreos, con el objetivo de mantener sistemas de información integrados.
- Mantener un inventario actualizado de equipos, en atención a las políticas vigentes en esta materia, para contar con información oportuna para la toma de decisiones y cumplir con la normativa institucional vigente.

Solución CA Services Desk Management

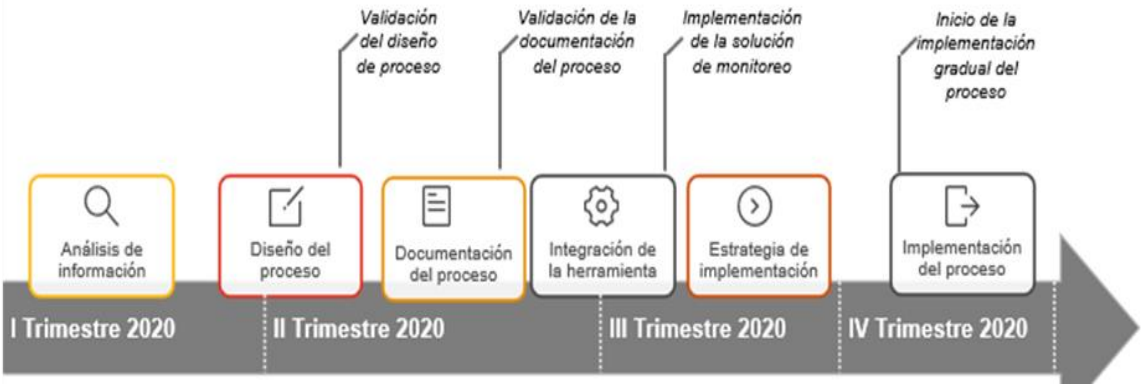
La herramienta CA Services Desk Management es una solución tecnológica utilizada para administrar los servicios de TI siguiendo un flujo de trabajo centralizado, sus principales características incluyen la gestión de procesos como las operaciones, configuración, cambios, disponibilidad y capacidad, activos, problemas, peticiones e incidentes, así como la aceptación y transición.

En lo que respecta al monitoreo de la Plataforma Tecnológica Central de la Caja Costarricense del Seguro Social, el 16 de enero de 2020, la Direccion de Tecnologías de Información y Comunicaciones mediante la Licitación Abreviada 2019LA-000012-1150 cuyo objeto es "*Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk Management",* adquirió servicios profesionales de integración con CA Services Desk Managment para monitorear los componentes tecnológicos según los siguientes Subítems:

- Subítem 1.1: Servicios para creación e implementación de procesos ITIL®.
- Subítem 1.2: Servicios profesionales a demanda para la integración de la herramienta de monitoreo resultante del Item II con CA Service Desk Management, y transferencia de conocimiento,
- Item 2: Solución de monitoreo de la Plataforma Tecnológica.

El desarrollo de ese proyecto contempló el análisis de información, diseño y documentación del proceso, integración de la herramienta, estrategia de implementación y finalmente la implementación del proceso, como se muestra en la siguiente imagen:

Figura N°2
Línea de tiempo del Proyecto de monitoreo de la Plataforma Tecnológica Central



Fuente: Información suministrada por la Direccion de Tecnologias de Información y Comunicaciones.

Según lo indicado por la administración activa, la herramienta de monitoreo efectúa revisiones de los equipos tecnológicos ubicados en CODISA y el piso 11 de Oficinas Centrales (servidores, equipos de seguridad, equipos de redes, soluciones de respaldo, balanceadores y Storage).

Productos de Auditoría

La Auditoría Interna en su función de Fiscalizadora ha emitido documentos vinculados con la gestión de la Plataforma Tecnológica Institucional, los cuales se detallan a continuación:

- **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.

  Respecto del Plan de Continuidad de Tecnologías de Información y Comunicaciones (TIC) si bien se dispone del documento actualizado y aprobado por las instancias correspondientes, aún no se han ejecutado pruebas a su efectividad ante una posible interrupción a causa de un evento negativo, por lo que se podría materializar el riesgo de no ejecutar las acciones correspondientes para mantener la continuidad de negocio en el momento oportuno.

  En ese mismo orden de ideas, la Administración no dispone de un enlace de redundancia en las telecomunicaciones instaladas en los edificios de la Dirección de Calificación de la Invalidez y La Casona las cuales permiten la transmisión de datos con el nivel central

- **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.

En el tema de activos, esta Auditoría evidenció debilidades en la identificación de licencias de software utilizadas para operar la Plataforma Tecnológica Central, por medio de placa institucional y registro en el Sistema Contable de Bienes Muebles (SCBM).

- **ATIC-21-2014: "***Evaluación integral sobre la gestión técnico-administrativa de la Dirección de Tecnologías de Información y Comunicaciones"*.

  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-330-2015:** Gestión de procesamiento y almacenamiento central de información efectuada por el Área de Soporte Técnico, específicamente de la Sub Área de Administración de Plataforma.
  Los resultados del estudio permitieron evidenciar la ausencia de indicadores de gestión de las actividades sustantivas ejecutadas, mecanismos para la rendición de cuentas a los niveles superiores, el incremento entre las operaciones y los recursos para la administración de la Plataforma Tecnológica Central.

  Por otra parte, se detectaron oportunidades de mejora referentes al cumplimiento de las funciones establecidas en el Manual de Organización de la Dirección de Tecnologías de Información y comunicaciones, la escalabilidad horizontal y vertical de los equipos informáticos de la plataforma supra citada, la estandarización de las solicitudes de pases a ambientes de producción capacitación y pruebas, así como el respaldo documental relacionado con el almacenamiento, borrado de archivos y respaldo y/o recuperación de datos de índole institucional.

- **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.

Asimismo, en lo que respecta de los mecanismos de contingencia para dicha Plataforma, se comprobó que el Plan de Continuidad en TIC del Área de Soporte Técnico no se actualiza desde su aprobación en el 2014, situación que podría comprometer la capacidad de respuesta ante eventos que limiten o inhabiliten los servicios tecnológicos que administra dicha unidad por medio del Centro de Cómputo Principal.

Finalmente, pese a los controles existentes para monitorear el funcionamiento de la Plataforma Tecnológica Central, a la fecha de elaboración del presente estudio, la Dirección de Tecnologías de Información y Comunicaciones no ha definido y oficializado los criterios que permitan determinar los rangos de funcionamiento óptimo de esos dispositivos, aspecto que podría comprometer la prestación oportuna de los servicios tecnológicos que brinda la institución al no disponer de los insumos necesarios que peritan anticipar condiciones adversas.

- **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 Sub Área 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 Sub Área Gestión de Producción, tales como: gestión de monitoreo y respaldos de la información en la Plataforma Tecnológica Central.

  Aunado a esto, se evidenciaron debilidades de seguridad lógica y que las actividades de monitoreo ejecutadas sobre la Plataforma Tecnológica Central no se encuentran disponibles bajo el horario de atención 24x7x365, lo anterior debido a que durante el 2015 se careció de labores de monitoreo durante 413 horas, lo cual representa un promedio de 41 horas al mes sin la supervisión constante de los operadores y analistas.

- **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.

Respecto a la administración del equipamiento no se realizan diagnósticos situacionales donde se valore el estado actual de la plataforma tecnológica que soporta las telecomunicaciones en los sitios, además, en lo que respecta a las inversiones para la adquisición de equipo y servicios, se observan acciones que no responden a las necesidades actuales que refieren las unidades.

- **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.

HALLAZGOS

1. SOBRE EL SITIO ALTERNO DE PROCESAMIENTO DE DATOS.

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.

Las Normas Técnicas para la gestión y control de las Tecnologías de Información (2007), establecen en los apartados 1.3 y 1.4.7, que:

> *"1.3 La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.*
>
> *"1.4.7 La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios (…)"*

Asimismo, el inciso 3.1 *"Consideraciones generales de la implementación de TI",* señala que:

> *"La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:*
> *(…)*
> *e. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.*
> *f. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio."*

Al respecto, el 19 de octubre de 2020, a través de entrevista efectuada al Máster Christian Chacón Rodríguez, Subdirector de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

> *"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.*
>
> *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 9 de setiembre de 2020, mediante entrevista efectuada al Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico, mencionó 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."

Además, el 2 de octubre de 2020, a través de entrevista efectuada al Máster Alexander Ordoñez Arroyo, Jefe de la Subárea de Administración de Plataformas, mencionó 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."

La ausencia de un sitio alterno de procesamiento de datos, el cual brindaría continuidad a las actividades sustantivas de la institución ante interrupciones provocadas por desastres naturales, problemas de funcionamiento de dispositivos, vulnerabilidades de seguridad, entre otros, podría ocasionar la materialización de riesgos asociados a la suspensión de los servicios brindados a los usuarios a través de la Plataforma Tecnológica Central como lo son atenciones en salud, procesos de recaudación, planillas, pensiones, entre otros.

Adicionalmente, podría generarse una pérdida de datos de salud y pensiones de la población en general provocando un impacto en la imagen de la Caja Costarricense del Seguro Social.

Sobre este particular, la Auditoria Interna durante los últimos siete años ha elaborado diferentes productos (informes y sus correspondientes seguimientos, así como oficios de advertencia) respecto a la importancia de que la Institución disponga de un sitio alterno para la continuidad de los servicios ante una eventualidad en el Centro de Datos Principal.

2. SOBRE EL PLAN DE CAPACIDAD DE LA PLATAFORMA TECNOLÓGICA CENTRAL

Esta Auditoría constató la ausencia de un plan de capacidad para la Plataforma Tecnológica Central, lo cual adquiere relevancia si se considera lo indicado al respecto en el documento *"Lineamientos para la definición de planes de capacidad en la plataforma central de tecnologías de información y comunicaciones (DTI-I-AP-0003)"*, el cual establece:

"…1. Presentación

*La gestión de la capacidad constituye un proceso que busca **asegurar que la operación de las tecnologías de información y comunicaciones en toda organización de trabajo, cumple satisfactoriamente con los requerimientos presentes y futuros que son demandados**. A medida que el uso de los servicios cambia y las funcionalidades para satisfacerlos evolucionan, se requiere que las capacidades de la infraestructura tecnológica que les soportan se adapten a las mismas.*

*Ante estas premisas, resulta vital el **establecimiento de acciones de control y planificación que faciliten la administración de procesos de mejora a la capacidad tecnológica de la***

***organización**, promoviendo con ello: la continuidad de operación de la infraestructura tecnológica, el rendimiento de los recursos bajo las calidades requeridas, la reducción de riesgos vinculados al proceso, el desarrollo de una cultura de trabajo proactiva.*

*En razón de lo anterior, **la Dirección de Tecnologías de Información y Comunicaciones mediante el Área de Soporte Técnico, define los lineamientos generales para la definición de planes de gestión de la capacidad sobre la plataforma institucional de tecnologías de información y comunicaciones**, lo que permita con ello asegurar que la capacidad y desempeño de los servicios tecnológicos y recursos que los soportan, se encuentren debidamente alineados a las necesidades existentes. (…)*

3. Introducción (…)

*Producto de la gestión de la capacidad que se realiza a la plataforma central TIC, se establece una serie de tareas que contribuyen a desarrollar distintas actividades para **mejorar diariamente su calidad**, entre los cuales es posible citar: la optimización de la plataforma configurando y balanceando cargas en los equipos, la valoración de nuevos requerimientos presentados ante el ingreso de nuevos servicios o funcionalidades, la evaluación de equipos de acuerdo a criterios establecidos para determinar su nivel reemplazo o mejora mediante la adquisición de componentes.*

*El resultado final del proceso de gestión de la capacidad, se encuentra definido a través del desarrollo de un plan de gestión de la capacidad, en cual se presentan las **necesidades técnicos de fortalecimiento y los elementos justificantes que les sustentan, constituyendo así un insumo fundamental para planificar el tema de la adquisición de equipamiento**, entre ellos: estudios de factibilidad, estudios de mercado, asignaciones de contenido presupuestario, proyectos de adquisición de equipos y/o mantenimiento, entre otros…".* El resaltado no corresponde al original.

De acuerdo con lo establecido en la norma anterior, el plan mencionado constituye un elemento primordial en la planificación de la adquisición de equipamiento, optimización de la calidad en la plataforma, establecimiento de medidas de control, mejora de la capacidad tecnológica, así como garantía del cumplimiento de los requerimientos presentes y futuros para operación de servicios y sistemas que dependen de dicha infraestructura.

Las Normas de Control Interno para el Sector Público (2009), en el Capítulo IV "*Normas sobre actividades de control*", específicamente en los apartados 4.1 *"Actividades de control*", 4.3 *"Protección y conservación del patrimonio"* y 4.5 *"Garantía de eficiencia y eficacia de las operaciones"*, se indica lo siguiente:

"4.1 Actividades de control

El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad.

El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la institución. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante.

4.3 Protección y conservación del patrimonio

El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales activos y los riesgos relevantes a los cuales puedan verse expuestos, así como los requisitos indicados en la norma 4.2.

4.5 Garantía de eficiencia y eficacia de las operaciones

El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas, así como los requisitos indicados en la norma 4.2."

Esas mismas Normas, en su apartado 5.9 *"Tecnologías de Información"*, señala:

"5.9 Tecnologías de Información

El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la CGR. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información."

Las Normas Técnicas para la gestión y control de Tecnologías de Información de la CGR (2007), en sus apartados 2.1 "*Planificación de las tecnologías de información"* y 2.3 "*Infraestructura tecnológica"*, indican respectivamente:

"2.1 Planificación de las tecnologías de información

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes (…)

(…)2.3 Infraestructura tecnológica

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI."

Esas mismas Normas, en su apartado 3.3 *"Implementación de infraestructura tecnológica"*, señala:

"La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual."

Asimismo, en su inciso 4.2 "*Administración y operación de la plataforma tecnológica"*, indica lo siguiente:

"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:
b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.

c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas." (El formato negrito y subrayado no corresponde al original)."

Los lineamientos para la definición de planes de capacidad en la Plataforma Tecnológica Central de Tecnologías de Información y Comunicaciones (2015), aprobados por el Máster José Willy Cortés, en el apartado 5.5 *"Sobre la documentación de planes de capacidad"*, hacen referencia a lo siguiente:

"5.5 Sobre la documentación de planes de capacidad

Constituye responsabilidad de la Jefatura del Área de Soporte Técnico:

a. Documentar formalmente planes de capacidad sobre la plataforma central TIC, de acuerdo con los resultados que se obtengan producto del análisis de los ámbitos técnicos de evaluación descritos en los apartados 6.2, 6.3 y 6.4 del presente documento, a saber:

- *Requerimientos del usuario.*
- *Monitoreo de plataforma central TIC.*
- *Evaluación del nivel de reemplazo de equipos.*

b. Abarcar el siguiente detalle de información en la documentación de planes de gestión de capacidad:

- *Servicio TIC involucrado.*
- *Detalle de equipos que deben ser reemplazados según servicio involucrado, considerando:*
  - ✓ *Número de placa*
  - ✓ *Costo unitario y total,*
  - ✓ *Partida presupuestaria afectada.*
  - ✓ *Justificación.*
- *Detalle de equipos que deben ser adquiridos para cada servicio, considerando:*
  - ✓ *Costo unitario y total*
  - ✓ *Partida presupuestaria afectada.*
  - ✓ *Justificación.*
- *Detalle de componentes que deben ser adquiridos para mejorar el desempeño y disponibilidad del servicio involucrado, considerando:*
  - ✓ *Costo unitario y total*
  - ✓ *Partida presupuestaria afectada.*
  - ✓ *Justificación.*
- *Detalle de propuesta sobre:*
  - ✓ *Virtualización.*
  - ✓ *Balanceo.*
  - ✓ *Continuidad del servicio.*
  - ✓ *Contrato de mantenimiento y costo. "*

El documento DTI-IST-0001 "*Esquema de la Continuidad de los Servicios Informáticos del Área de Soporte Técnico" aprobado por el Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico el 20 de agosto de 2018 mediante el oficio DTIC-5386-2018*, en el punto N°5 *"El Plan de Capacidad"*, menciona lo siguiente:

> *"**5. El Plan de Capacidad***
>
> *Es un registro donde con los recursos disponibles y con la retroalimentación en primera instancia de los usuarios finales, se elabora una proyección de los requerimientos de hardware y software para satisfacer la demanda de servicio en un tiempo que define la Administración. De existir poca o ninguna retroalimentación del usuario final, con la ayuda de la experiencia acumulada, se elabora la proyección de recursos a futuro con el objetivo de planear los proyectos que van a satisfacer la demanda de aplicaciones y/o servicios al usuarios. (sic)*
>
> *Lo anterior es un estudio que dará un resultado aproximado por lo que existe el riesgo asociado."*

Sobre este tema, mediante entrevista efectuada el 30 de octubre de 2020, el Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

> *"Si bien es cierto no se dispone de un plan integral sobre la Capacidad de equipos de la Plataforma Tecnológica Central, actualmente las unidades de la Dirección de Tecnologías de Información desarrollan de manera individual actividades de monitoreo constante de la Plataforma Tecnológica Central con el objetivo de visualizar comportamientos de crecimiento, identificando situaciones que podrían requerir renovación tecnológica e indicando sus necesidades a través de los planes operativos con la finalidad de realizar la renovación de los componentes por cuanto no se tiene un Plan de Capacidad formalmente definido, no obstante, este aspecto se pretende mejorar a través de procesos de la gestión de TIC."*

En ese mismo orden de ideas, el 19 de octubre de 2020, a través de entrevista efectuada al Máster Christian Chacón Rodríguez, Subdirector de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

> *"Finalmente, si bien es cierto el proyecto ya se finalizó, actualmente no tenemos implementado al 100% un proceso de gestión de la capacidad, el cual ya está por operativizarse, de hecho, actualmente se está finalizando la implementación del Plan de Capacidad que se encuentra en la fase de implementación y definición de roles."*

Además, el 23 de junio de 2020, mediante el oficio DTIC3631-2020, el Máster Jorge Sibaja Alpízar indicó lo siguiente:

> *"En la actualidad el proceso de capacidad de la plataforma se realiza de forma manual, utilizando las estimaciones de crecimiento que se generan en la plataforma y los requerimientos que se reciben de unidades externa a la DTIC."*

Adicionalmente, el 9 de setiembre de 2020, mediante entrevista efectuada, el Máster Sibaja, señaló lo siguiente:

> *"El proceso para la realización de estudios formales está en desarrollo. Sin embargo, se realizan estudios con los datos que se obtienen de la capacidad y uso de la plataforma y con la información de crecimiento anual de los servicios. Además, se considera la demanda recibida."*

Aunado a esto, el Máster Alexander Ordoñez Arroyo, Jefe de la Subárea de Administración a la Plataforma, en entrevista efectuada el 5 de octubre de 2020, indicó lo siguiente:

> *"Actualmente no se dispone de un plan de capacidad para la planificación de necesidades de la plataforma tecnológica central, se tiene gestión de capacidad controlando el crecimiento de la plataforma, cada vez que se hace una compra se realiza un pequeño estudio donde se revisa el consumo y las solicitudes de los usuarios, por ejemplo, el personal de bases de datos me indica*

como está el crecimiento de la base de datos y que ocupa. Sobre este tema cuesta mucho tener información referente a los usuarios, los nuevos proyectos y las estimaciones de la capacidad requerida, asimismo, como parte de la compra de la herramienta de monitoreo se incluyó la ejecución de un proceso de plan de capacidad con la definición de servicios de capacidad y gestión de incidencias.

Hace un tiempo intentamos implementar un Plan de Capacidad, pero era muy difícil porque no tenemos la información de todos los insumos asociados a las necesidades de los usuarios sobre la proyección de lo que ocupan en un tiempo definido para realizar la compra de insumos, lo que se hace es una gestión de capacidad conforme al estado del equipo y el crecimiento que tuvo durante el año y se planifica para el otro año o las necesidades que tenemos, ahorita con la compra que se está realizando se va a implementar el Plan de Capacidad,.."

No disponer del plan integral de capacidad de los equipos que soportan las operaciones y transacciones de las soluciones utilizadas en la prestación de servicios y las bases de datos institucionales, limita las acciones de la administración en torno a la toma de decisiones estratégicas en temas como planificación, direccionamiento e inversión en TIC, así como estimaciones del crecimiento de la información y usuarios. Lo anterior, podría ocasionar la materialización de riesgos vinculados con la continuidad de servicios, afectaciones en los tiempos de respuesta de la infraestructura tecnológica ante la implementación de nuevos requerimientos en detrimento de los servicios tecnológicos brindados.

Al respecto, resulta relevante disponer de un instrumento formalmente establecido para la determinación del estado de la Plataforma Tecnológica Central institucional, permitiendo la retroalimentación respecto a la adquisición de hardware y software requeridos para la demanda de servicios TIC, respaldando las erogaciones monetarias destinadas para el fortalecimiento de la Plataforma de marras.

Llama la atención que la Administración no disponga de este plan, considerando la importancia de este instrumento para la gestión de la plataforma, así como el monto de las inversiones asociadas a la infraestructura tecnológica central por el orden de los $15 millones en los últimos siete años.

3. SOBRE EL PLAN DE CONTINUIDAD DE LOS SERVICIOS INSTITUCIONALES

Esta Auditoría identificó aspectos de mejora en torno a la continuidad en la prestación de los servicios de la Caja Costarricense de Seguro Social a través de la disponibilidad de la Plataforma Tecnológica Central, los cuales se mencionan a continuación:

3.1 Sobre la ejecución de pruebas integrales para verificar la continuidad de los servicios brindados mediante la Plataforma Tecnológica Central

Se constató la ausencia de planificación y ejecución de pruebas integrales para verificar la continuidad de las actividades sustantivas institucionales gestionadas a través de la Plataforma Tecnológica Central con la participación de los responsables de los procesos de las unidades de negocio y la Dirección de Tecnologías de Información y Comunicaciones (administradores de las soluciones tecnológicas), lo anterior, considerando elementos de disponibilidad de los componentes tecnológicos.

Las Normas técnicas para la gestión y control de las Tecnologías de Información (2007), en el Capítulo III *"Implementación de las tecnologías de información"*, específicamente en el inciso 1.4.7 *"Continuidad de los servicios de TI"*, señalan lo siguiente:

"1.4.7 Continuidad de los servicios de TI

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias

con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."

Esas mismas normas en el apartado 3.1 *"Consideraciones generales de la Implementación de TI"*, hace referencia a lo siguiente:

*"**3.1 Consideraciones generales de la implementación de TI***
La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: (…)

c. Garantizar la participación de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas."

El Manual para elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones ASCI-UCG-ORG-002, Versión 2.4- mayo de 2013, específicamente en los apartados *"Ensayos de Simulación"* y *"Frecuencia de los ensayos"*, menciona lo siguiente:

*"**Ensayos de Simulación***

Establecer escenarios para los ensayos ante un desastre, los cuales provean a los participantes con situaciones que podrían afectar como cada miembro de los equipos reaccionará. Los escenarios brindarán a la administración con una base para iniciar la activación de sus planes y efectuar la recuperación de los procesos de negocios de los cuales ellos son responsables.

Frecuencia de los ensayos

Los ensayos deben ser realizados al menos una vez al año, o en su defecto de los cambios en el ambiente en las operaciones. No obstante, dependiendo del riesgo, es conveniente elaborar un calendario de ensayos más frecuente y riguroso. Es conveniente tener en cuenta que los resultados de los ensayos deben ser formalmente reportados. Además, en caso de que sea necesario, el Plan podría requerir ser actualizado, para lo cual el CPC debe actualizar un formulario "Mantenimiento del Plan" (PTC014) incluido en esta guía."

Sobre este tema, el 30 de octubre de 2020, mediante entrevista efectuada al Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

"Efectivamente no se están realizando simulacros para verificar de manera conjunta el Plan de Continuidad y disponibilidad para todos los servicios, lo anterior teniendo en cuenta que el de continuidad le corresponde al negocio y el de disponibilidad a la Dirección de Tecnologías de Información y Comunicaciones.

Así mismo, los simulacros deberían partir de un análisis de riesgos y ser del parte del proceso de disponibilidad, el cual, como se indicó se encuentra en fase de implementación. Si hablamos de componentes tecnológicos entraría el proceso de disponibilidad donde nosotros deberíamos hacer esos simulacros que no existen actualmente, por lo cual con el desarrollo del proceso de disponibilidad este tema será abarcado. Por otra parte, como mencioné anteriormente, el plan de continuidad involucra al negocio ya que abarca más que las acciones de TIC y la Caja Costarricense de Seguro Social actualmente no tiene un Plan de Continuidad definido formalmente para realizar los simulacros, al menos que yo conozca."

Aunado a este, el Máster Christian Chacón Rodríguez, Subdirector de Tecnologías de Información y Comunicaciones mediante entrevista efectuada el 19 de octubre de 2020, mencionó lo siguiente:

"En realidad, primero quisiera aclarar los conceptos de disponibilidad que se refiere a componentes de TI y continuidad asociado a los componentes de negocio, en realidad tecnologías de información podría participar en un plan de continuidad del negocio como apoyo técnico pero lo que nosotros deberíamos hacer es pruebas de disponibilidad del servicio que es nuestra competencia al 100% según las mejores prácticas. Respecto a la disponibilidad, no quisiéramos verlo solo enfocado a pruebas de los equipos sino a servicios tecnológicos como el correo electrónico, navegación, SICERE y EDUS. En vista de lo anterior, actualmente no estamos realizando pruebas de disponibilidad para el servicio tecnológico. Como les mencioné anteriormente, nos encontramos finalizando los procesos de capacidad, eventos y disponibilidad, en este último la idea es empezar a realizar esos ejercicios de disponibilidad de los servicios tecnológicos.

Para referirme específicamente a la pregunta sobre la continuidad, por ejemplo, si la Contraloría plantea que el SICERE tiene pruebas de continuidad, a nivel de negocio no lo conozco, siendo que este se basa en una plataforma tecnológica, sin un sitio alterno difícilmente se podrían realizar las pruebas. Por otra parte, tengo conocimiento que existen esfuerzos desde la Dirección SICERE y la Gerencia Financiera en conjunto con la Dirección de Tecnologías de información y Comunicaciones para que, con el proyecto de sitio alterno se realice primero la viabilidad técnica y una vez lista, nos podríamos mover en conjunto con el negocio para realizar las pruebas de continuidad de los servicios.

Como lo mencionaba hace un momento, si hoy fallara SICERE, se deben establecer ciertos aspectos relacionados con la definición del encargado a nivel de negocio de trasladarlo al sitio alterno o si debiera ser de forma automática, un rol del negocio donde se indique el momento de efectuar el traslado, los ejercicios de simulacro y las pruebas a realizar a nivel de negocio. Lo que se ha hecho es tratar de mitigar riesgos, por lo cual en conjunto con el negocio tenemos un reunión mensual donde además de ver incidentes y otros aspectos a nivel del servicio de recaudación y SICERE, realizamos pruebas para poder tener contingencia en caso de una eventualidad, replicando en el piso 11 del edificio Jenaro Valverde Marín las bases de datos del EDUS y SICERE ubicadas en las instalaciones de CODISA, esto lo hacemos utilizando un software gratuito de Oracle denominado Data Guard, el cual permite realizar la replicación de los datos de forma pasiva-activa.."

Aunado a lo anterior, el 9 de setiembre de 2020, mediante entrevista efectuada al Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico, mencionó lo siguiente:

"La forma de realizar los simulacros es mediante la continua actualización de la plataforma, ya que para mantener la continuidad de los servicios se actualizan todos los sistemas (Servidores, Switches, Storage, balanceadores, entre los mas importantes.). en general todos los entornos productivos están construidos sobre ambientes en alta disponibilidad, esto es clúster físicos y virtuales o granjas de clúster o granjas de Servidores.

Por ejemplo: Las bases de datos, están soportadas en clúster físicos y algunas en clúster virtuales, y cada vez que hay una actualización ya sea de la base de datos, del Sistema Operativo o del firmware de las maquinas o de virtualización se aplica siempre sobre uno de los componentes mientras el otro soporta los servicios y una vez que se ha realizado la actualización del primero, se pasan los servicios, al actualizado y se actualiza el otro componente, luego se balancea de nuevo. Este proceso se repite para prácticamente todos los componentes. Actualmente se realiza para Switches de SAN y para los Storage's V9000 y V5030.

La contingencia actual es principalmente a través de componentes en alta disponibilidad y algunos recursos en el Cuarto de Comunicaciones del Piso 11."

Además, el 2 de octubre de 2020, mediante entrevista efectuada al Master Alexander Ordoñez Arroyo, Jefe de la Subárea de Administración de Plataformas, indicó lo siguiente:

> *"No se efectúan simulacros o pruebas para verificar el funcionamiento del plan de contingencia porque la CCSS no tiene sitio alterno, lo que existe es una pequeña réplica de ciertas bases de datos (EDUS, SICERE y MISE) en el piso 11 del Edificio Jenaro Valverde, Por otra parte, si se tiene redundancia y alta disponibilidad de todos los equipos por ejemplo si un servidor de base de datos o un balanceados fallan se tiene otro igual en CODISA, además, en ese sitio un rack se alimenta de dos fuentes diferentes, pero sitio alterno no hay y ese proceso se tendría que ver directamente con la Dirección de Tecnologías de Información de Comunicaciones porque ese tema si está fuera de mi alcance.*
> *Para que se ejecute un simulacro de verificación del plan de contingencia se debe tener todos los componentes de plataforma duplicados (base de datos, servidores de aplicaciones de servicios de Microsoft, el Active Directory, entre otros) para poder realizar las pruebas correspondientes."*

Además, el 29 de octubre de 2020, a través de entrevista realizada al Lic. Geiner Gamboa Otárola, Jefe de la Subárea de Gestión de la Producción, hizo referencia a lo siguiente:

> *"Nosotros no podemos realizar ensayos del Plan de Continuidad por cuanto no podemos apagar equipos interrumpiendo los servicios, en cuanto a la contingencia se mantienen varios aspectos por ejemplo para la mayoría de equipo critico tenemos uno similar como respaldo, también, existe un sistema de respaldos de datos donde se mantiene copias diarias (en forma electrónica) de las bases de datos"*

La planificación y ejecución de pruebas integrales para garantizar continuidad a los servicios brindados a través de la disponibilidad de la Plataforma Tecnológica Central, le permitiría a la institución prepararse y valorar como responder ante la materialización de riesgos en torno a las posibles interrupciones en la operación producto de eventos fortuitos, de la naturaleza, así como incidentes de diferentes magnitudes. Adicionalmente, la realización de este tipo de actividades facilitaría los procesos de recuperación o el restablecimiento de las condiciones normales, en caso de que se presente una contingencia real.

Por otra parte, el no efectuar este tipo de actividades podría generarle limitaciones vinculadas con la valoración de tiempos de respuesta, capacidad de reacción institucional articulada del negocio con TI, con el fin de conocer el impacto en la afectación de la prestación de servicios críticos y operativos en situaciones reales.

3.2. Sobre el cumplimiento de las directrices en el Plan de Continuidad para la gestión en TIC del Área de Soporte Técnico

Si bien es cierto, la administración dispone del documento PCGTIC-AST-001 denominado Plan de Continuidad para la gestión en TIC del Área de Soporte Técnico aprobado por el Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico el 22 de agosto de 2018, evaluado el 30 de agosto de 2018 por el Lic. Leonardo Fernández Mora, Jefe de la Subárea de Continuidad de la Gestión, se detectaron las siguientes oportunidades de mejora:

- El plan se encuentra desactualizado desde agosto de 2018, es decir han transcurrido más de dos años desde su última modificación.
- Se detectó una inconsistencia entre la fecha consignada en el historial de revisiones del documento de marras correspondiente al 24 de setiembre de 2014 y la identificada en el Informe sobre la Evaluación del Plan de la Gestión de TIC del Área de Soporte Técnico, emitido el 30 de agosto de 2018 por el Lic. Fernández Mora.
- Asimismo, no se visualiza en el documento remitido a este Órgano de Fiscalización y Control las firmas de revisión y la aprobación por cada uno de los responsables establecidos, aspectos fundamentales en el proceso de formalización y acatamiento.

Las Normas Técnicas para la Gestión y Gestión de las TIC (2007) establecen en su apartado 1.4.7 *"Continuidad de los servicios de TI"*, lo siguiente:

> *"La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.".

Las Políticas de Seguridad Informática institucionales (2007) establecen en su apartado 10.14 *"Política para la elaboración de Planes de Continuidad de la Gestión"*, lo siguiente:

"Los Planes de Continuidad de la Gestión, deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. Adicionalmente como los planes de continuidad de la gestión pueden fallar debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, debe considerarse dentro de su administración la realización de pruebas periódicas para garantizar que los mismos estén actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.".

Sobre esta temática, si bien es cierto el Máster Chacón Rodríguez, Subdirector de Tecnologías de Información y Comunicaciones mediante entrevista efectuada el 19 de octubre de 2020, indica que la competencia de Dirección se asocia a la ejecución de pruebas de disponibilidad del servicio según las mejores prácticas y la continuidad corresponde a los dueños del negocio, al momento de efectuar el presente estudio no se ha establecido formalmente un plan de disponibilidad de los componentes tecnológicos que permitan la sostenibilidad de los procesos del negocio ante eventualidades relacionadas con la Infraestructura Tecnológica Central, la cual administra el software y hardware requerido para la prestación de los servicios ofrecidos por la institución.

Sobre el Plan de Continuidad del Área de Soporte Técnico, el 9 de setiembre de 2020, mediante entrevista realizada al Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico, indicó lo siguiente:

"Si está documentado. Requiere actualización. Y además el proceso de disponibilidad dará la atención integral a este tema."

Adicionalmente, el 29 de octubre de 2020, mediante entrevista efectuada al Lic. Geiner Gamboa Otárola, Jefe de la Subárea de Gestión de la Producción, mencionó lo siguiente:

"Yo colaboro a don Jorge Sibaja con la conformación del Plan de Continuidad y el que tenemos es el del 2018, lo anterior debido a que no se ha podido actualizar por cuanto se han tenido que realizar diferentes actividades lo cual no nos ha permitido efectuar la actualización respectiva de este documento"

La falta de controles respecto a la verificación del cumplimiento de la normativa vigente aplicable asociada al Plan de Continuidad del Área de Soporte Técnico podría comprometer el correcto funcionamiento de los servicios brindados por esa unidad para la atención de los usuarios, patronos y pensionados del Seguro de Enfermedad y Maternidad (SEM) y del Régimen de Invalidez, Vejez y Muerte (IVM).

La situación descrita podría comprometer la continuidad de los servicios que brinda la Plataforma Tecnológica Central ante la materialización de eventos como desastres, siniestros y fallas que limiten o inhabiliten su funcionamiento adecuado, en detrimento de la atención asegurados, patronos, pensionados y demás usuarios de los servicios del Seguro de Enfermedad y Maternidad (SEM) y del Régimen de Invalidez, Vejez y Muerte (IVM).

4. SOBRE EL PLAN DE REEMPLAZO DE LOS ACTIVOS QUE CONFORMAN LA PLATAFORMA TECNOLÓGICA CENTRAL

Según la información analizada, se determinó la ausencia de un plan integral de reemplazo de los activos que conforman la Plataforma Tecnológica Central, el cual incluya aspectos de valor agregado tales como:

- Criticidad y uso de los activos.
- Criterios para la valoración de las sustituciones.
- Relación costo-beneficio en la reparación o mejora tecnológica.
- Capacidad de efectuar mejorados tecnológicas.
- Garantías vigentes y contratos de mantenimiento.
- Disponibilidad de insumos y repuestos.
- Soporte de fabricante.

Lo anterior adquiere relevancia en virtud de lo mencionado en el documento "*Lineamientos Generales de inventarios TIC (TIC-INV-0001)"*, donde se establece:

> *"Presentación*
>
> *La implementación de estos lineamientos conlleva una serie de beneficios para la Institución, entre ellos, mantener un inventario de los recursos tecnológicos, su estado, condiciones, visibilidad del uso y propiedad de los activos de tecnologías de información.* ***Con ello, se pretende crear consciencia en la administración activa de la necesidad de realizar una adecuada planeación presupuestaria e inversión en recursos de tecnologías de información*** *(…)*
>
> *(…) Introducción*
>
> *Hoy día, toda unidad de trabajo requiere de la utilización de las tecnologías de información y comunicaciones (TIC) para la prestación de los servicios, ya sea a usuarios internos o externos a la Institución. Como tal,* ***debe planificar su adquisición, mantenimiento, mejora, reemplazo o desecho según los lineamientos establecidos por la Dirección de Tecnologías de Información y Comunicaciones (DTIC). Es por ello, que este documento presenta lineamientos generales que ayudaran a conocer las responsabilidades en la gestión de los activos de tecnologías de información, así como establecer los mecanismos e instrumentos con que se cuentan para su administración y gestión*** *(…)*
>
> *(…) Además, se señalan lineamientos para la revisión periódica de los activos de TIC.* ***Será a través de la implementación de un programa de revisiones o diagnóstico que los Centros de Gestión Informática mediante el instrumento Guía de Reemplazo de Equipo de a conocer a las autoridades del centro de trabajo las necesidades de remplazo, desecho, reparación y mejora de los recursos de TI.*** *Su aplicación y efectividad es una responsabilidad compartida entre la administración de los centros de trabajo y los encargados del Centros de Gestión Informática respectivo, quien presta soporte y asesoría a dicha unidad de trabajo. Todo ello, se complementa al esfuerzo que se debe realizar en los centros de trabajo, con el fin de conocer las nuevas necesidades en materia de recursos de tecnologías de información, de tal forma que la administración de los centros de trabajo pueda planificar su adquisición, mejora o reparación en los ejercicios presupuestarios y de planificación operativa.*
>
> ***La efectividad en la implementación de los lineamientos establecidos en este documento permitirá planificar el desarrollo tecnológico de las unidades de trabajo, según las políticas establecidas para consolidar sistemas de información integrados y robustos, así como contar con una plataforma tecnológica establece y alineada al modelo de infraestructura tecnológica que se impulsa en la Institución****.". (El subrayado y la negrita no corresponden al texto original)*

Las Normas Técnicas para la gestión y control de Tecnologías de Información de la CGR (2007), en sus apartados 2.1 *"Planificación de las tecnologías de información"* y 2.3 *"Infraestructura tecnológica"*, indican respectivamente:

> *"2.1 Planificación de las tecnologías de información*
>
> *La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes (…)*
>
> *(…)2.3 Infraestructura tecnológica*
> *La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI."*

Esas mismas Normas, en su apartado 3.3 *"Implementación de infraestructura tecnológica"*, señala:

> *"La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual."*

Asimismo, en su inciso 4.2 *"Administración y operación de la plataforma tecnológica"*, indica lo siguiente:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
> *c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas." (El formato negrito y subrayado no corresponde al original).*

Los Lineamientos Generales de Inventario TIC TIC–INV-0001(2011), versión 1.0.0, en su apartado 8 "Responsabilidad sobre la reparación", mejora o remplazo de los recursos TIC indica lo siguiente:

> *"Es responsabilidad de la autoridad del centro de trabajo, con base en el Informe de Remplazo, planificar conforme las regulaciones institucionales la reparación, mejora o remplazo de los recursos de TI, girando las instrucciones pertinentes a los encargados de los distintos procesos*

Sobre esta temática, el 30 de octubre de 2020, mediante entrevista efectuada al Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, indicó lo siguiente:

> *"Si efectivamente no existe un plan de Remplazo de la Plataforma Tecnológica Central de manera formal, porque no se tiene implementado el proceso de capacidad, sin embargo, cada jefatura genera sus necesidades de acuerdo con la información que dispone. En ese sentido, se consideran las recomendaciones de fabricantes, la obsolescencia tecnológica, soporte, tendencias de mercado, la ejecución de diversos análisis y procesos como el de gestión de activos, y el Plan de Capacidad que es un insumo generador de información para dicha planificación, siendo que estos últimos dos están pendientes de implementar."*

Además, el 9 de setiembre de 2020, mediante entrevista efectuada al Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico, mencionó lo siguiente:

"Se dispone de un procedimiento interno que establece criterios para el reemplazo de equipos."

Aunado a esto, el 3 de octubre de 2020, mediante entrevista al Máster Alexander Ordoñez Arroyo, Jefe de la Subárea de Administración de Plataformas, señaló lo siguiente:

> *"Actualmente no se tiene un plan de remplazo de equipos en la Subárea a mi cargo por cuanto resulta difícil la ejecución debido a limitantes en torno a los presupuestos asignados para este tipo de actividades de sustitución de equipos y que estos tienen diferentes garantías según el modelo o la marca, el tiempo de garantía y soporte por el proveedor, por lo cual dificulta la definición de fechas estimadas para realizar el cambio. Actualmente se va a incluir un proceso denominado Gestión de Activos, en el cual se va a reforzar el control de la depreciación o estado de vida útil de los componentes de la Plataforma Tecnológica Central.*
>
> *Sobre este tema, se considera adecuada la sustitución una vez finalizada la garantía ofrecida por el proveedor para no incurrir en costos adicionales por conceptos de adquisición de servicios de mantenimientos posteriores."*

La elaboración de un plan de remplazo de los componentes de la Plataforma Tecnológica Central permitirá a la administración activa realizar proyecciones sobre las inversiones en la adquisición de componentes durante un periodo determinado, lo anterior con el objetivo de minimizar la materialización de riesgos en torno a fallas en los equipos, en detrimento de los servicios brindados.

Adicionalmente, la Institución se expone a pérdida de información de los usuarios por fallas, así como el incremento de los costos por concepto de mantenimiento y reparación de equipos.

En ese sentido, la ausencia de planificación de reemplazo de los activos podría ocasionar eventual fraccionamiento en materia de contratación, afectando economías de escala y de proceso.

5. SOBRE LA OBSOLESCENCIA DE LOS EQUIPOS QUE CONFORMAN LA PLATAFORMA TECNOLÓGICA CENTRAL

De conformidad con los datos registrados en el Sistema Contable de Bienes Muebles (SCBM) respecto a la vida útil de 233 activos que conforman la Plataforma Tecnológica Central a cargo de la Dirección de Tecnologías de Información y Comunicaciones (el detalle se incluyó en el Anexo N°1), se determinaron los siguientes aspectos:

- 49 activos correspondientes al 21,03%, se encuentran totalmente depreciados, situación que se torna relevante por cuanto son equipos tecnológicos utilizados para la gestión de soluciones institucionales críticas e información sensible requerida para la prestación de los servicios.
- 106 bienes concernientes al 45,49% de los componentes tienen una vida útil del 50% o inferior.
- 78 elementos tienen una vida útil superior al 51%.
- Adicionalmente, no se identificó una valoración de riesgos en torno a la obsolescencia tecnológica, vulnerabilidades de seguridad, imposibilidad de brindar soporte técnico por el fabricante, problemas en torno a la actualización requerida a través del tiempo, entre otros.

Las Normas Técnicas para la gestión y control de la Tecnologías de Información y Comunicaciones de la CGR (2007), en su apartado 3.3 *"Implementación de infraestructura tecnológica"*, señala:

> *"La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual."*

Así mismo, en su inciso 4.2 *"Administración y operación de la plataforma tecnológica"*, indica lo siguiente:

"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:
b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas." (El formato negrito y subrayado no corresponde al original).

A criterio de este Órgano de Fiscalización y Control, la situación descrita anteriormente podría obedecer a la ausencia del Plan de reemplazo de activos TIC, el cual debería considerar dentro de sus criterios la vida útil de estos dispositivos, lo anterior en acatamiento de la normativa vigente aplicable.

La utilización de activos de tecnologías de información y comunicaciones que ya agotaron su vida útil o se encuentran en un porcentaje avanzado de depreciación, puede comprometer la continuidad de los procesos críticos de la Caja Costarricense de Seguro Social, lo anterior, por cuanto los equipos con niveles considerables de obsolescencia son propensos a presentar fallas en su funcionamiento, además, las empresas fabricantes limitan el soporte de hardware y software en virtud de su evolución, lo cual dificulta la obtención de repuestos e insumos compatibles con esos equipos, así como su correspondiente mantenimiento.

6. SOBRE LOS INFORMES DE GESTION EMITIDOS POR EL ÁREA DE SOPORTE TÉCNICO

De conformidad con la información analizada en torno a los informes emitidos por el Área de Soporte Técnico respecto a la gestión de los procesos y servicios, se determinaron los siguientes aspectos:

6.1 Sobre la rendición de cuentas respecto a la gestión de la plataforma tecnológica central

Respecto al proceso de rendición de cuentas mensual del Área de Soporte Técnico a la Dirección de Tecnologías de Información y Comunicaciones en torno a las actividades relacionadas con la Plataforma Tecnológica Central, se detectó lo siguiente:

- No se identificó la validación de indicadores relacionados con la gestión de procesos de la Plataforma Tecnológica Central para la toma de decisiones por parte de la Dirección de Tecnologías de Información y Comunicaciones.
- Aunado a lo anterior, no se visualizó respaldo documental referente al proceso de retroalimentación por parte del Área de Soporte Técnico hacía las subáreas a su cargo, lo anterior basado en los resultados emitidos por los diferentes servicios.
- No se visualizó un proceso formalmente definido respecto a la validación del cumplimiento de las metas de las diversas subáreas por parte del Área de Soporte Técnico, incluyendo la participación de la Subárea del Aseguramiento de la Calidad desde el rol de asesor.

La Constitución Política de la República de Costa Rica (2015), específicamente en el Artículo 11, hace referencia a lo siguiente:

"ARTÍCULO 11.-Los funcionarios públicos son simples depositarios de la autoridad. Están obligados a cumplir los deberes que la ley les impone y no pueden arrogarse facultades no concedidas en ella. Deben prestar juramento de observar y cumplir esta Constitución y las leyes. La acción para exigirles la responsabilidad penal por sus actos es pública. La Administración Pública en sentido amplio, estará sometida a un procedimiento de evaluación de resultados y rendición de cuentas, con la consecuente responsabilidad personal para los funcionarios en el cumplimiento de sus deberes. La ley señalará los medios para que este control de resultados y rendición de cuentas opere como un sistema que cubra todas las instituciones públicas. "

La Ley General de Control Interno N° 8292, en el Artículo N°10- *"Responsabilidad por el sistema de control interno"*, hace referencia a lo siguiente:

*"**Artículo 10 Responsabilidad por el sistema de control interno.***

Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento."

Ese mismo cuerpo normativo en el Artículo N°17 *"Seguimiento del sistema de control interno"*, menciona lo siguiente:

*"**Artículo 17 —Seguimiento del sistema de control interno**.*

Entiéndese por seguimiento del sistema de control interno las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo; asimismo, para asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud.

En cuanto al seguimiento del sistema de control interno, serán deberes del jerarca y los titulares subordinados, los siguientes:

a) Que los funcionarios responsabilizados realicen continuamente las acciones de control y prevención en el curso de las operaciones normales integradas a tales acciones."

Las Normas de Control Interno para el Sector Público (2009), en el Capítulo I *"Normas Generales"*, precisamente en el inciso N°1.7 *"Rendición de Cuentas"*, indica:

*"**1.7 Rendición de cuentas sobre el SCI***

1.7 El jerarca y los titulares subordinados, según sus competencias, deben disponer y ejecutar un proceso periódico, formal y oportuno de rendición de cuentas sobre el diseño, el funcionamiento, la evaluación y el perfeccionamiento del SCI ante los diversos sujetos interesados."

Además, esas mismas Normas en el Capítulo IV *"Normas sobre actividades de Control Interno"*, específicamente en el apartado 4.5.1 *"Supervisión constante"*, menciona lo siguiente:

*"**4.5.1 Supervisión constante***

El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos."

Las Normas técnicas para la gestión y control de la Tecnologías de Información de la CGR (2007), en el Capítulo IV, específicamente en los incisos 5,1 y 5,2, establece lo siguiente:

*"**5.1 Seguimiento de los procesos de TI***

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

5.2 Seguimiento y evaluación del control interno en TI

> El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas.*"*

Al respecto, mediante entrevista efectuada el 30 de octubre de 2020, el Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

> *"Respecto a la validación de los indicadores, actualmente no se está realizando para esos procesos. Para los ya implementados, asimismo, hay un proceso adicional en desarrollo denominado Sistema de Gestión de Calidad, el cual se enfoca en el nivel de madurez de implementación de cada proceso, en esa misma línea hemos gestionado una plaza para un ingeniero industrial con el objetivo de agilizar estos procesos de validación, mientras tanto vamos trabajándolo con el recurso actual."*

Por otra parte, el 9 de setiembre de 2020, mediante entrevista realizada al Máster Jorge Sibaja Alpízar, Jefe del Área de Soporte Técnico, respecto a esta temática, señaló lo siguiente:

> *"Para los incidentes existe el proceso de gestión de incidentes y peticiones. Para problemas existe el proceso de gestión de problemas. Para todas las situaciones que se presentan, se tienen grupos de WhatsApp, donde cualquier situación se atiende por múltiples involucrados, incluidos el Señor Director y el Señor Subdirector. Por otra parte, y para atender este tema integralmente se desarrollan los procesos de Gestión de Eventos (Todo lo que pasa), gestión de la Capacidad (Planificación de la capacidad requerida) y gestión de la disponibilidad (cualquier evento que refleja una situación de que afecta o podría afectar los servicios). Estos procesos responderán a estas preguntas de manera formal."*

Aunado a esto, a través de entrevista efectuada el 13 de octubre de 2020, el Máster Mario Vilchez Moreira, indicó lo siguiente:

> *"La Subárea de Aseguramiento de la Calidad aún no tiene la tarea de verificar el cumplimiento de los diversos indicadores asociados al proceso de la Plataforma Tecnológica Central. No contamos con todos los indicadores. En los últimos años nos hemos abocado a realizar un acompañamiento en el diseño e implementación de los procesos que conforman el modelo de gestión de servicios TIC. Los informes de desempeño se generan y se trasladan a las jefaturas de Área y ellos a la Dirección. La Subárea colabora en el diseño e implementación del DashBoard. El modelo aún no se encuentra maduro, se encuentra en proceso de implementación."*

El no definir formalmente un proceso de rendición de cuentas donde se establezca entre otros aspectos las metas de cumplimiento de las diversas actividades vinculadas con la gestión de la Plataforma Tecnológica Central, podría materializar riesgos asociados al incumplimiento de los objetivos propuestos, limitaciones en torno a la revisión y validación de avances en un periodo establecido, la identificación de posibles oportunidades de mejora, desviaciones o atrasos, la retroalimentación por parte de la Direccion de Tecnologías de Información y Comunicaciones hacia las unidades encargadas de la Plataforma de marras, lecciones aprendidas, entre otros.

6.2 Sobre la gestión de minutas correspondientes a sesiones de trabajo entre la Dirección de Tecnologías de Información y Comunicaciones y el Área de Soporte Técnico.

De conformidad con la revisión efectuada de las minutas correspondientes a las sesiones de trabajo entre la Dirección de Tecnologías de Información y Comunicaciones y el Área de Soporte Técnico durante el periodo comprendido entre febrero y octubre de 2020, se identificó los siguientes aspectos:

- Solamente se obtuvo el respaldo documental de las sesiones de trabajo concernientes a febrero, abril y mayo de 2020.

- No se identificó información vinculada con la revisión de los informes de gestión de los procesos emitidos mensualmente por el Área de Soporte que permitieran constatar el análisis de los resultados, la definición de oportunidades de mejora y la respectiva retroalimentación.
- No se identificó el seguimiento por parte de la administración activa al cumplimiento de los acuerdos definidos en reuniones previas.
- En lo que respecta a las reuniones efectuadas el 14 de febrero y el 8 de mayo de 2020, no se visualizan las firmas de los participantes, asimismo, las minutas correspondientes a las sesiones de trabajo del 3 y el 8 de abril de 2020, incompletitud en la totalidad de las rubricas de los funcionarios, aspectos que no permite evidenciar su asistencia.

La Ley General de Control Interno N° 8292, específicamente en el Artículo N° 10 *"Responsabilidad por el Sistema de Control Interno"*, hace referencia a lo siguiente:

> *"Artículo 10 —Responsabilidad por el sistema de control interno.*
>
> *Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento."*

Las Normas de Control Interno para el Sector Público (2009), en el Capítulo IV *"Normas sobre Actividades de Control"*, establece lo siguiente:

> *"4.5.2 Gestión de proyectos. El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.*
>
> *Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:*
>
> *"(…) c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.*
> *d El establecimiento de un sistema de información confiable, oportuna, relevante y competente para dar seguimiento al proyecto…""*

La ausencia del respaldo documental asociado a la revisión de los informes de rendición de cuentas de la gestión de la Plataforma Tecnológica Central por parte de la Dirección de Tecnologías de Información y Comunicaciones podría generar limitaciones en torno a identificación de los temas tratados y el análisis de los resultados emitidos en un periodo determinado, los acuerdos definidos y el correspondiente seguimiento para validar su cumplimiento, así como la identificación y aplicación de oportunidades de mejora detectadas.

7. SOBRE LAS MÉTRICAS ESTABLECIDAS EN LA HERRAMIENTA CA SERVICES DESK MANAGEMENT PARA EL MONITOREO DE LA PLATAFORMA TECNOLÓGICA CENTRAL

De conformidad con la revisión del respaldo documental correspondiente a la definición de métricas para la gestión del monitoreo del estado de la memoria, CPU y rendimiento de los equipos que componen la Plataforma Tecnológica Central específicamente de los servidores de aplicaciones, balanceadores de cargas, sistemas de almacenamiento, respaldos, seguridad y WWAN, lo anterior a través de la herramienta CA Services Desk Management, se identificaron los siguientes aspectos:

- Las valores asociados a las métricas de marras fueron definidas por funcionarios de la Dirección de Tecnologías de Información y Comunicaciones y remitidos a la Máster Adriana Moreira Madrigal, encargada del proyecto de la Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk Management, mediante correos electrónicos, sin que se confeccionaran documentos formalmente aprobados para la identificación de estos umbrales con información relevante sobre el origen de estos datos.
- No se dispone de respaldo documental asociado a la revisión, validación y aprobación de los valores mencionados en correos electrónicos por el nivel superior correspondiente, así como su oficialización al personal a cargo de la parte operativa.

La ley General de Control Interno N°8292, en el Artículo N°16 *"Sistemas de información",* se indica lo siguiente:

> *"En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:*
>
> *a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.*
>
> *b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficiente de los recursos públicos."*

Las Norma de Control Interno para el Sector Público (2009), en el inciso 1.1. *"Sistema de Control Interno",* menciona lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben emprender las medidas pertinentes para contar con un SCI, conformado por una serie de acciones diseñadas y ejecutadas por la administración activa para proporcionar una seguridad razonable en la consecución de los objetivos organizacionales."*

Esas Normas en el apartado 1.2 *"Objetivos del SCI"*, en el inciso C. *"Garantizar eficiencia y eficacia de las operaciones",* determina lo siguiente:

> *"c. Garantizar eficiencia y eficacia de las operaciones. El SCI debe coadyuvar a que la organización utilice sus recursos de manera óptima, y a que sus operaciones contribuyan con el logro de los objetivos institucionales."*

Sobre este tema, el 7 de octubre de 2020, mediante entrevista efectuada a la Máster Adriana Moreira Madrigal, funcionaria de la Dirección de Tecnologías de Información y Comunicaciones a cargo de la Administración del Proyecto *"Solución de Monitoreo para la Plataforma Tecnológica Central, desarrollo de procesos ITIL y Servicios de Integración de herramientas con CA Services Desk",* indicó lo siguiente*:*

> *"Los umbrales y/o métricas implementadas en la solución de monitoreo corresponden a criterios técnicos del personal experto de las diferentes áreas de la Dirección de Tecnologías de Información y Comunicaciones, que se han construido producto de su conocimiento y trabajo diario con las herramientas. Estas métricas aportadas son usadas hoy en día como parte de las labores operativas de estos equipos técnicos, algunas de ellas ya forman parte de las herramientas de cada equipo físico, así como de las recomendaciones de los fabricantes de los mismos, constituyéndose en información técnica operativa.*
>
> *El establecer métricas corresponden a un tema meramente técnico y no administrativo. La DTIC cuenta con personal especializado para establecer dichas métricas, que son las que se han implementado en la solución como base, ya que la misma solución de monitoreo contempla una*

variedad importante de métricas que genera propiamente con base en la información que recolecta producto del monitoreo; así mismo como se indicó incluso algunos de estos umbrales ya están definidos por el fabricante de los equipos, de manera tal que la mismas no requieren de un aval administrativo. Ahora bien, para conocer cuál fue el método utilizado por cada uno de los equipos técnicos, deberá consultarse a cada área que conforma la DTIC, ya que para el Proyecto de Monitoreo se consultó a los equipos técnicos expertos la base requerida."

La falta de definición formal de indicadores para gestionar el monitoreo de la Plataforma Tecnológica Central con la correspondiente revisión, aprobación y oficialización de estos valores por parte del Nivel Superior podría limitar la toma de decisiones asociadas al funcionamiento de la PTC, así como la aplicación de mejoras continuas a las métricas implementadas. Además, se podrían materializar riesgos asociados a la identificación de los umbrales establecidos, entre otros por el desconocimiento de personal debido a la falta de socialización de estos.

8. SOBRE LA CONTRATACIÓN DEL SERVICIO DE HOSPEDAJE PARA EL CENTRO DE DATOS PRINCIPAL DE LA INSTITUCIÓN EN EL MARCO DEL PROYECTO DE FORTALECIMIENTO DE LA ARQUITECTURA DE LA PLATAFORMA TECNOLÓGICA CENTRAL

De conformidad con el respaldo documental relacionado con la contratación del hospedaje para el Centro de Cómputo Principal, se determinaron los siguientes aspectos:

8.1 Sobre la vigencia del contrato actual para Albergar el Centro de Cómputo Principal de la CCSS.

Según la revisión documental del contrato N° 002-2017, relacionado con la Licitación Pública 2017LN-000001-1150 cuyo objeto es *"Servicio de Hospedaje para Albergar el Centro de Cómputo Principal de la CCSS"*, se determinó que al 30 de octubre de 2020 no se había publicado el cartel licitatorio para dar inicio al nuevo proceso contractual, lo anterior toma relevancia por cuanto la fecha de finalización de la última prórroga de la Licitación de marras finaliza el 17 de agosto de 2021.

El Reglamente a la Ley de Contratación Administrativa, en el Capítulo VII *"Tipos de procedimientos"*, Sección Primera, Licitación Pública, específicamente en el Artículo N°95 *"Adjudicación y Readjudicación"*, señala lo siguiente:

"La licitación deberá ser adjudicada dentro del plazo previsto en el cartel, que en ningún caso podrá ser superior al doble del plazo fijado para recibir ofertas.

El plazo para adjudicar podrá ser prorrogado por un tanto igual al indicado en el cartel, para lo cual deberá mediar resolución motivada suscrita por el Proveedor. En ella, además de valorarse las razones que originan la prórroga, se contemplará el ajuste de los plazos de los cronogramas.
Vencido el plazo original más su prórroga, cuando ésta se hubiere dado, sin que se haya dictado el acto de adjudicación, los oferentes tendrán derecho a dejar sin efecto su propuesta y a que de inmediato se les devuelva la garantía de participación, sin que les resulte aplicable sanción alguna por esa razón. Asimismo, los funcionarios responsables del no dictado oportuno del acto de adjudicación estarán sujetos a las sanciones previstas en los artículos 96 y 96 bis de la Ley de Contratación Administrativa."

Las Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR (2007), en el Capítulo III *"Implementación de las tecnologías de información"*, específicamente en el inciso 3.1 *"Consideraciones generales de la implementación de TI"*, señala lo siguiente:

"3.1 ***Consideraciones generales de la implementación de TI***

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: (..)

(…) g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos."

Al respecto, mediante entrevista efectuada el 30 de octubre de 2020, el Máter Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, mencionó lo siguiente:

"Actualmente, nuestra idea es publicar el cartel para una nueva Licitación antes de finalizar el 2020, el cual es muy similar al del proceso anterior. En este momento, el aspecto que nos está atrasando es el aval por parte de la Comisión de Egreso y Gasto, por lo tanto, voy a consultarle al Gerente Financiero don Luis Diego Calderón sobre el tema."

Aunado a lo anterior, el Lic. Geiner Gamboa Otárola, Jefe de la Subárea de Gestión de la Producción, a través de entrevista realizada el 28 de octubre de 2020, indicó lo siguiente:

"Actualmente el cartel de la nueva licitación se encuentra al 90%, de hecho, el 9 de octubre envié el estudio de mercado para que los proveedores coticen el precio para la nueva contratación y en el momento que la obtenga seria cuestión de un mes para trasladar el respaldo documental a la Subarea de Compras y que se proceda con las revisiones para continuar con el proceso contractual para la adquisición de los servicios para albergar el Centro de Cómputo Principal.

Finalmente, por ser un proceso un poco complejo se le envió la documentación sobre la solicitud de precios a los proveedores con suficiente tiempo y en este momento estoy esperando sus respuestas."

El tiempo disponible para efectuar el proceso licitatorio de la contratación del hospedaje del Centro de Cómputo Principal de la CCSS, podría limitar la participación de potenciales oferentes en virtud de los plazos requeridos para las actividades asociadas al traslado de los componentes actualmente ubicados en el Parque Tecnológico en CODISA, a una eventual nueva sede, en caso de contratar otro proveedor diferente a Ideas Gloris S.A.

***8.2* Sobre la eventual dependencia con el proveedor de servicios Ideas Gloris S.A.**

Se determinó que la Caja Costarricense de Seguro Social ha venido adquiriendo el Servicio para Hospedaje del Centro de Cómputo Principal desde el 2009 hasta la fecha con la empresa Ideas Gloris S.A., cuyo Parque Tecnológico se encuentra ubicado en CODISA, según el siguiente detalle:

- Mediante Contrato 004-2009 se adjudicó el proceso contractual No. 2009CD-000002-1150 a la empresa Ideas Gloris S.A., a partir del 14 de agosto de 2009 por 12 meses con prórroga por cuatro años.
- En misiva N° DCA-0208 (01222) del 26 de enero del 2016, la Contraloría General de la República autorizó una prórroga del contrato 004-2009, por un periodo de 18 meses a partir del 18 de febrero del 2016.
- A través de Contrato N°002-2017, se adquirieron nuevamente los servicios del proveedor Ideas Gloris S.A para albergar el Centro de Cómputo Principal de la CCSS, por un periodo de 12 meses, a partir del 17 de agosto de 2017 con la posibilidad de realizar prorrogas hasta por tres años máximo.

Adicionalmente, este Órgano de Fiscalización y Control no identificó un estudio en el cual se valorarán aspectos técnicos, funcionales, operativos, económicos y legales, que permita a la administración activa analizar alternativas para promover la independencia de proveedores de servicios en el sitio de procesamiento de datos y los escenarios ante posibles traslados de la Infraestructura Tecnológica Central.

Aunado a lo anterior, llama la atención de esta Auditoría Interna lo identificado en el documento *"Informe de Avance respecto al Proyecto de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Central (Centro de Datos), emitido por la Dirección de Tecnologías de Información y Comunicaciones"*, en el cual se contempló

el Parque Tecnológico en CODISA como Sitio Principal de Procesamiento de Datos o Alterno en aproximadamente seis oportunidades.

Las Normas técnicas para la gestión y control de las Tecnologías de Información de la CGR (2009), en el Capítulo III *"Implementación de tecnologías de información"*, específicamente en el inciso 3.1 *"Consideraciones generales de la implementación de TI"*, se indica lo siguiente:

> *"**3.1 Consideraciones generales de la implementación de TI***
>
> *" La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: (…)*
>
> *(…) i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios.*

Esas mismas Normas, en su apartado, 4.6 *"Administracion de servicios prestados por terceros"*, indica lo siguiente:

> *"La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe: (…)*
>
> *(…) d. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero."*

8.3 Sobre la gestión de riesgos asociada a la adquisición del Servicio para Hospedar el Centro de Cómputo Principal de la CCSS

Se determinó que la administración no ha efectuado actividades en torno a la valoración formal de riesgos inherentes al Servicio para Hospedar el Centro de Cómputo Principal, el cual incluya temas como posibles atrasos en el procedimiento de contratación, continuidad del negocio, análisis financiero de los servicios contratados, participación de potenciales oferentes, así como un plan de tratamiento en caso de materialización de vulnerabilidades, entre otros.

La Ley General de Control Interno N°8292, en el Artículo N°2- *"Definiciones"*, inciso f, hace referencia a lo siguiente:

> *"f) **Valoración del riesgo:***
>
> *Identificación y análisis de los riesgos que enfrenta la institución, tanto de fuentes internas como externas relevantes para la consecución de los objetivos; deben ser realizados por el jerarca y los titulares subordinados, con el fin de determinar cómo se deben administrar dichos riesgos."*

Esa misma Ley, en el Artículo N°14 *"Valoración del riesgo"*, específicamente en los incisos b y d, indica lo siguiente:

> *"Artículo 14. —**Valoración del riesgo**. En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:*
>
> *b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.*
>
> *d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar."*

Las Normas de Control Interno para el Sector Público (2009), en el Capítulo III *"Normas sobre valoración del riesgo"*, en el inciso 3.1 "Valoración del Riesgo", indica lo siguiente:

*"**3.1 Valoración del riesgo***

El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure."

Además, esas Normas en el Capítulo IV "*Normas sobre actividades de Control"*, inciso 4.3 *"Protección y conservación del patrimonio"*, señalan lo siguiente:

"4.3 Protección y conservación del patrimonio

El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales activos y los riesgos relevantes a los cuales puedan verse expuestos, así como los requisitos indicados en la norma 4.2."

Las Normas Técnicas para la gestión y control de las Tecnologias de Información (2007), en el apartado 1.3 *"Gestión de Riesgos"*, menciona lo siguiente:

"1.3 Gestión de Riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."

Esas mismas Normas, en el punto 1.4.7 *"Continuidad de los servicios de TIC"*, hacer referencia a lo siguiente:

*"**1.4.7 Continuidad de los servicios de TIC***

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

*Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, **la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad**." (la negrita y subrayado no corresponde al texto original)*

Adicionalmente, en el inciso 3.1 *"Consideraciones generales de la implementación de TI"*, hace referencia a lo siguiente:

*"**3.1 Consideraciones generales de la implementación de TI***

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: (…)

(…) g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.

i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios"

Al respecto, el Máster Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones, a través de entrevista efectuada el 30 de octubre de 2020, mencionó lo siguiente:

> *"Finalmente, no se ha efectuado una valoración de riesgos vinculados con posibles atrasos en la tramitación de la licitación para Albergar el Centro de Cómputo Principal de la CCSS u otros, por lo cual se podría trabajar en un plan donde se consideren diversos escenarios y posteriormente identificar riesgos asociados con el respaldo documental correspondiente."*

El no efectuar una evaluación y análisis de los riesgos asociados a la adquisición de servicios de terceros para albergar el Centro de Cómputo Principal de la Caja Costarricense de Seguro Social, podría ocasionar su materialización, minimizando la posibilidad de la Institución de prevenir aspectos vinculados con el detrimento de sus finanzas ante la eventual elevación del precio definido por el proveedor para la prestación de ese tipo de servicios, interrupción de los servicios críticos ante el finalización de operaciones de la empresa contratada, daños de los equipos traslados a otras instalaciones, entre otros.

Finalmente, esta Auditoría Interna ha emitido diversos productos vinculados con temas relacionaos a la contratación del servicio de hospedaje de los componentes tecnológicos del Centro de Cómputo Principal, en los cuales se han mencionado aspectos de mejora asociados a la planificación y ejecución de dicha solución por parte de la administración activa, los cuales se observan a continuación:

- ATIC-393-2010: La Administración no ha establecido una estrategia para el resguardo del Centro de Cómputo Principal luego de finalizado el contrato de arrendamiento señalado.
- AD-ATIC-29934-2013: Oficio referente a la valoración de alternativas en torno a la contratación del hospedaje para el Centro de Datos Principal.
- AD-ATIC-38000-2014 Finalización del Contrato 004-2009 *"Servicio de hospedaje para albergar el Centro de Cómputo Principal (CCP) de la CCSS"*.
- ATIC-154-2014: La institución no define una estrategia para disponer del servicio de hospedaje del Centro de Cómputo Principal (CCP) a largo plazo (señalado en el informe ATIC-393-2010 y oficio DCA-1899 (resolución N° 07318) en el cual la Contraloría General de República autoriza la ampliación del contrato 004-2009 por un período de 18 meses a partir de la finalización de la prórroga vigente).
- ATIC-26-2017: Se comprobó que el contrato N° 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"*, finaliza el 17 de agosto del 2017, y aún la Institución no dispone de una estrategia para albergar la plataforma tecnológica central posterior a esta fecha.

CONCLUSIONES

La infraestructura tecnológica de una institución le permite soportar las soluciones de negocios y la gestión administrativa para la ejecución de sus actividades sustantivas, en ese sentido, la Caja Costarricense de Seguro Social, a través de su plataforma brinda servicios de salud, pensiones, aseguramiento, recaudación y otros a la ciudadanía. De igual forma, las funcionalidades administrativas, financieras, de ofimática y colaborativos en general, son soportados por componentes de hardware y software, la cual debe estar preparada y acorde con los requerimientos de operación, rendimiento y seguridad entre otros. Lo anterior con el objetivo de que los usuarios y la ciudadanía reciban servicios oportunos y de calidad.

Al respecto, es necesario que la Caja disponga de una estrategia integral de gestión de la Plataforma Tecnológica Central, que le permita no solo la continuidad y calidad de sus prestaciones, sino también se efectúe un mejor aprovechamiento de los recursos institucionales, con un enfoque de sostenibilidad y disponibilidad que apoyen las decisiones sobre la ruta tecnológica establecida, mediante los estudios pertinentes que debe realizar.

Lo anterior, considerando las inversiones que ha realizado la Institución en los últimos seis años por más de $15,861,634 (quince millones ochocientos sesenta y un mil dólares con 00/100), así como la dependencia para su funcionamiento, de las unidades de negocio tanto de misión crítica como de apoyo administrativo, de esa infraestructura,

Es preciso que la planificación, ejecución, seguimiento y evaluación de los proyectos alrededor de la PTC, no solo respondan a las estrategias y prioridades institucionales, sino también se alineen y complementen sistemáticamente entre ellas, para alcanzar los objetivos planteados. Por ello, es necesario también generar los mecanismos de aprobación y conocimiento del Consejo Tecnológico en aras de lograr el acompañamiento y apoyo requerido.

Asimismo, el fortalecimiento de los mecanismos de rendición de cuentas contribuirá con el logro de los objetivos que la Caja defina en esa materia, no solo a lo interno de la Dirección de Tecnologías de Información, sino también ante la Gerencia General y Órganos Colegiados respectivos, todo esto en total consonancia con el Modelo Meta de Gobierno de las TIC y de los instrumentos formales de planificación.
En ese orden de ideas, disponer del Plan de Capacidad de la Plataforma Tecnológica y del Plan de reemplazo de activos que conforman la PTC formalizados y aprobados, permitirían a la Institución responder de manera planificada a las necesidades de funcionalidad, crecimiento y rendimiento de los equipos y dispositivos en general, aportando insumos para la toma de decisiones en la planificación de inversiones tanto a corto como mediano y largo plazo, de conformidad con las posibilidades financieras, propiciando un ambiente de control que contribuya con la disponibilidad y continuidad del servicio.

En ese sentido, resulta fundamental la actualización del Modelo de Infraestructura Tecnológica, el cual también contribuiría con el establecimiento del rumbo tecnológico por el cual debe transitar la Institución.

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.

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.

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

1. En alineamiento con las iniciativas derivadas a partir de la implementación del Modelo Meta de Gobernanza de las TIC y de la Seguridad de la Información aprobado, así como los proyectos y líneas de acción estratégicos, establecidas en la Agenda Digital Institucional (AGEDI), conformar un equipo interdisciplinario a cargo de la revisión y diagnóstico de las causas que propiciaron la materialización de los riesgos identificados por esta Auditoría Interna, la cual permita obtener el insumo necesario para definir y ejecutar una estrategia integral para el fortalecimiento de la gestión de la Plataforma Tecnológica Central (PTC) con

el fin de evitar a futuro, la presentación de las vulnerabilidades detectadas en el presente informe, contemplando al menos los siguientes aspectos:

- Gestión de la capacidad y disponibilidad del hardware y software que conforma la PTC según lo mencionado en hallazgo dos del presente informe.
- Ejecución periódica de pruebas de disponibilidad de la PTC en coordinación con las unidades usuarias de conformidad con el marco normativo vigente y lo señalado en ellos hallazgos 3.1 y 3.2.
- Análisis y planificación del reemplazo de los activos que conforman la PTC durante un periodo establecido de conformidad con la normativa vigente aplicable y lo señalado en los hallazgos cuatro y cinco.
- Mecanismos de rendición de cuentas respecto a la gestión de los procesos asociados a la PTC considerando lo indicado en los hallazgos 6.1 y 6.2.
- Gestión de los riesgos asociados al procesamiento y hospedaje del Centro de Cómputo Principal y Alterno, así como la eventual dependencia por parte de la institución con los proveedores que brindan dicho servicio de conformidad con lo mencionado en los hallazgos 8.1, 8.2 y 8.3.
- Actualización y socialización de los documentos que contribuyen en la gestión integral de la PTC.
- Revisión, análisis y actualización (de considerarse conveniente) de la vigencia del marco normativo vigente relacionado con la gestión integral de la Plataforma Tecnológica Central.
- Mecanismos de control para el monitoreo integral de la gestión de la PTC, así como la inclusión de acuerdos de niveles de servicio.
- Planificación, control y evaluación de las adquisiciones e inversiones asociadas a la gestión de la PTC de modo que, al gestionar las aprobaciones, la instancia correspondiente disponga del panorama general que le permita tomar decisiones en un ambiente de sostenibilidad y en total alineamiento con las estrategias institucionales.

Posteriormente, se deberá presentar la estrategia de marras ante el Consejo Tecnológico, en su rol responsable de la toma de decisiones estratégicas y seguimiento de los temas relacionados con las TIC, rindiendo cuentas sobre los riesgos materializados en la gestión de la PTC, así como la inclusión de las medidas de control adoptadas para evitar que las situaciones identificadas se presenten nuevamente.

Además, se deben justificar las medidas incluidas en dicha estrategia, con el fin de obtener el aval correspondiente para su ejecución. Igualmente, es necesario garantizar la participación de los Centros de Gestión Informática y demás unidades involucradas, con la finalidad de alinear los esfuerzos de TIC vinculados con esta temática.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a esta Auditoría en un plazo de seis meses a partir de la fecha de recepción del presente informe, la documentación que respalde las acciones ejecutadas por esa Dirección en torno a la revisión y diagnóstico de las causas que propiciaron la materialización de los riesgos identificados, la aprobación de la estrategia integral de la gestión PTC en los términos requeridos en la presente recomendación.

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:

0. Antecedentes relacionados con la valoración de los escenarios para el hospedaje y procesamiento del Sitio de Cómputo Principal y Alterno de la PTC.
1. Análisis de Factibilidad realizado a cada alternativa, así como la gestión de riesgos identificados.
2. Recomendación de la alternativa a criterio de la Dirección de Tecnologías de Información y Comunicaciones justificando los criterios utilizados en ese sentido.
3. Estado de la Licitación Pública 2017LN-000001-1150 *"Servicio de Hospedaje para Albergar el Centro de Cómputo Principal"*
4. 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.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 10 de diciembre de 2020 con el Master Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones y el Máster Christian Chacón Rodríguez, Subdirector de la DTIC.

A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

Sobre los Hallazgos: No hay observaciones sobre los hallazgos, no obstante, el Máster Robert Picado Mora, Subgerente de la Tecnologías de Información y Comunicaciones y el Máster Christian Chacón Rodríguez, Subdirector de la DTIC, solicitan la remisión del respaldo documental vinculado con la vida útil de los activos de la Plataforma Tecnológica Central. Asimismo, comentan los esfuerzos que se han llevado a cabo en torno a la gestión de los procesos de la Plataforma Tecnológica Central según el marco de referencia de ITIL.

Sobre las recomendaciones:

Recomendación 1:

El Máster Robert Picado Mora, subgerente de TIC solicita se sustituya el siguiente párrafo *"Revisión de la vigencia del marco normativo vinculado con la gestión integral de la PTC"* por el siguiente:

> *"Revisión, análisis y actualización (de considerarse conveniente) de la vigencia del marco normativo vigente relacionado con la gestión integral de la Plataforma Tecnológica Central"*

El Máster Christian Chacón Rodríguez solicita que se modifique el párrafo:

> *"Ejecución periódica de pruebas de continuidad de la PTC en coordinación con las unidades usuarias de conformidad con el marco normativo vigente y lo señalado en ellos hallazgos 3.1 y 3.2."*

Por el siguiente:

> *"Ejecución periódica de pruebas de disponibilidad de la PTC en coordinación con las unidades usuarias de conformidad con el marco normativo vigente y lo señalado en ellos hallazgos 3.1 y 3.2."*

Al respecto, se realiza el análisis vinculado con las solicitudes de modificación y se acogen los cambios en la recomendación supra cita.

Sobre el tiempo definido para la presentación de las acciones ejecutadas por parte de la Dirección de Tecnologías de Información y Comunicaciones en atención a la recomendación N°1, se estableció inicialmente un plazo de cuatro meses, sin embargo, el Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones solicita se incremente a seis meses.

En virtud de lo anterior, se analiza el tiempo solicitado y se incluye la modificación a un plazo de seis meses.

Recomendación 2:

La Máster Idannia Mata Serrano, Asistente de Auditoría, solicitó se incluya en el párrafo "Estado de la Licitación Pública 2017LN-000001-1150 "Servicio de Hospedaje para Albergar el Centro de Cómputo Principal", la siguiente información "y la valoración de los riesgos asociados."

Se acuerda, incluir en la redacción el cambio solicitado por la Máster Mata Serrano.

No se presentan observaciones vinculadas con el plazo otorgado para la atención de la oportunidad de mejora N°2.

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

IDANNIA MATA SERRANO (FIRMA)
Firmado digitalmente por IDANNIA MATA SERRANO (FIRMA)
Fecha: 2020.12.11 10:17:53 -06'00'

Máster Idannia Mata Serrano
Asistente de Auditoría

GRACE MONGE PICADO (FIRMA)
Firmado digitalmente por GRACE MONGE PICADO (FIRMA)
Fecha: 2020.12.11 10:28:59 -06'00'

Ing. Grace Monge Picado
Asistente de Auditoría

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2020.12.11 10:43:04 -06'00'

Lic. Rafel A. Herrera Mora
Jefe de Área

RAMH/IMS/GMP/ams

Anexo N°1

Vida útil de los activos que conforman la Plataforma Tecnológica Central a cargo de la Dirección de Tecnologías de Información y Comunicaciones.

Número placa	Descripción del activo	Porcentaje de vida útil
718592	MONITOR PARA COMPUTADORA LCD DE 17 "	0%
824432	MONITOR LCD CD 17"	0%
810712	SWITCH 4500 PWR 26 PUERTOS	0%
834197	CONVERTIDOR SIP-H 323, MARCA TANDBERT VIDEO COMMUNICATION SERVER 100 REGISTROS.	0%
834196	SERVIDOR DE VIDEOCOMUNICACION PARA PC, MOVI 15 USUARIOS. MARCA TANDBERG MODELO MOVI SERVER .	0%
986982	HP 3 PAR STORE SERV 7400	0%
986981	HP 3 PAR STORE SERV 7400	0%
986980	SISTEMA HP 3 PAR STORE SERV.7400	0%
849541	SERVIDOR HP INTEGRITY RX6600	0%
849538	SERVIDOR HP INTEGRITY RX6600	0%
849537	SERVIDOR HP INTEGRITY RX6600	0%
849536	SERVIDOR HP INTEGRITY RX6600	0%
849529	SERVIDOR HP PROLIANT DL380	0%
849528	SERVIDOR HP PROLIANT DL380	0%
849525	SERVIDOR HP INTEGRITY RX6600	0%
849519	SWITCH DIRECTOR HP	0%
849518	SWITCH DIRECTOR HP	0%
849517	GABINETE HP 10642 G2	0%
849516	GABINETE HP 10642 G2	0%
849514	GABINETE HP 10642 G2	0%
849512	GABINETE HP 10642 G2	0%
849511	GABINETE HP 10642 G2	0%
849510	GABINETE HP 10642 G2	0%
849509	GABINETE HP 10642 G2	0%
849508	GABINETE HP 10642 G2	0%

849506	GABINETE HP 10642 G2	0%
849505	GABINETE HP 10642 G2	0%
849504	GABINETE HP 10642 G2	0%
849503	GABINETE HP 10642 G2	0%
849502	GABINETE HP 10642 G2	0%
848466	SERVIDOR HP BLADE	0%
848462	SERVIDOR HP BLADE	0%
848459	SERVIDOR HP BLADE	0%
848458	SERVIDOR HP BLADE	0%
848454	SERVIDOR HP INTEGRITY RX6600	0%
848453	SERVIDOR HP INTEGRITY RX6600	0%
848452	SERVIDOR HP INTEGRITY RX6600	0%
824488	SERVIDOR BLADE HP PROLIANT	0%
824473	SERVIDOR BLADE HP PROLIANT	0%
858880	EQUIPO PARA COMUNICACION INALÁMBRICA, BH 300MBPS CONECTORIZADO 5.7 GHZ LINK	0%
858878	EQUIPO PARA COMUNICACION INALÁMBRICA, BH 300MBPS CONECTORIZADO 5.7 GHZ LINK	0%
986983	HP 3 PAR STORE SERV 7200	0%
824477	SERVIDOR BLADE HP PROLIANT	0%
759286	SERVIDOR SUN FIRE (SOLUCION PARA EL PROCESAMIENTO DE LA CAPA DE APLICACIONES WEB EN LA CCSS)	0%
679078	SERVIDOR HP MOD 380G4	0%
744938	EQUIPO PARA APLICACIONES ANTISPAM PARA FILTRADO DE CORREO ELECTRONICO BARRACUDAS SPAM FIREWALL	0%
744937	EQUIPO PARA APLICACIONES ANTISPAM PARA FILTRADO DE CORREO ELECTRONICO BARRACUDAS SPAM FIREWALL	0%
848486	SWITCH CISCO NEXUS 7000	0%
848485	SWITCH CISCO NEXUS 7000	0%
701177	ENRUTADOR CISCO 3745	22%
1148594	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148593	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148592	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148591	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148590	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148589	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148588	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148582	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148581	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148580	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148579	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148578	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148577	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148576	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148570	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148569	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148568	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148567	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%

1148566	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148565	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148564	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148558	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148557	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148556	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148555	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148554	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148553	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148552	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148543	BLADES LENOVO IBM FLEX SYSTEM ENTERPRISE CHASIS	40%
1148544	BLADES LENOVO IBM FLEX SYSTEM ENTERPRISE CHASIS	40%
1148545	BLADES LENOVO IBM FLEX SYSTEM ENTERPRISE CHASIS	40%
1148546	BLADES LENOVO IBM FLEX SYSTEM ENTERPRISE CHASIS	40%
1148573	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148587	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148586	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148585	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148584	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148583	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148575	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148574	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148547	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148572	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148571	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148563	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148562	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148561	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148560	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148559	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148551	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148550	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148549	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1148548	LENOVO FLEX SYSTEM X240 M5 COMPUTE NODE	40%
1150969	SERVIDOR PARA VCENTER SYSTEM X3550 M5	40%
986986	SERVIDOR DE CONSOLA PARA STORAGE SYSTEM X3250 M5	40%
1150971	MDS 9396S 96X16G FC 16 GBPS FC	40%
1150972	MDS 9396S 96X16G FC 16 GBPS FC	40%
1150970	SISTEMA DE ALMACENAMIENTO STORWISE V7000	40%
848500	SERVIDOR DE MEDIANA COMPLEJIDAD (EMPRESARIAL O DEPARTAMENTAL) COLOR NEGRO CON PLATEADO.	41%
809446	ENRUTADOR MARCA CISCO	41%
1157154	ENRUTADOR DE ALTA CAPACIDAD, MARCA CISCO, COLOR GRIS OSCURO	43%
1157156	SWITCHES CAPA DE DISTRIBUCIÓN MARCA CISCO, COLOR AZUL OSCURO	43%
1177717	SWITCH DE CAPA DE CORE, MARCA CISCO, COLOR GRIS	45%
1177716	SWITCH DE CAPA DE CORE, MARCA CISCO, COLOR GRIS	45%
1174001	SERVIDOR TIPO BLADE	46%

1174002	SERVIDOR TIPO BLADE	46%
1174003	SERVIDOR TIPO BLADE	46%
1174004	SERVIDOR TIPO BLADE	46%
1174005	SERVIDOR TIPO BLADE	46%
1174006	SERVIDOR TIPO BLADE	46%
1174007	SERVIDOR TIPO BLADE	46%
1174008	SERVIDOR TIPO BLADE	46%
1174034	SAN SWITCH MDS9396S.	46%
1174035	SAN SWITCH MDS9396S.	46%
1174033	FLEX SYSTEM ENTERPRISE CHASIS	46%
1174032	FLEX SYSTEM ENTERPRISE CHASIS	46%
1174031	FLEX SYSTEM ENTERPRISE CHASIS	46%
1174016	SERVIDOR TIPO BLADE	46%
1174015	SERVIDOR TIPO BLADE	46%
1174014	SERVIDOR TIPO BLADE	46%
1174013	SERVIDOR TIPO BLADE	46%
1174030	SERVIDOR TIPO BLADE	46%
1174029	SERVIDOR TIPO BLADE	46%
1174028	SERVIDOR TIPO BLADE	46%
1174027	SERVIDOR TIPO BLADE	46%
1174026	SERVIDOR TIPO BLADE	46%
1174025	SERVIDOR TIPO BLADE	46%
1174024	SERVIDOR TIPO BLADE	46%
1174023	SERVIDOR TIPO BLADE	46%
1174021	SERVIDOR TIPO BLADE	46%
1174020	SERVIDOR TIPO BLADE	46%
1174019	SERVIDOR TIPO BLADE	46%
1174017	SERVIDOR TIPO BLADE	46%
1174018	SERVIDOR TIPO BLADE	46%
1174009	SERVIDOR TIPO BLADE	46%
1174010	SERVIDOR TIPO BLADE	46%
1174012	SERVIDOR TIPO BLADE	46%
1174011	SERVIDOR TIPO BLADE	46%
1174022	SERVIDOR TIPO BLADE	46%
1172104	CONMUTADOR 10 GB ETHERNET, CISCO 4500X, COLOR GRIS	46%
1172103	CONMUTADOR 10 GB ETHERNET, CISCO 4500X, COLOR GRIS	46%
1172101	CONTROLADOR INALÁMBRICO, CISCO 5520, COLOR GRIS	46%
1172102	CONTROLADOR INALÁMBRICO, CISCO 5520, COLOR GRIS	46%
1180460	CONMUTADOR 10 GB ETHERNET CISCO 3650, COLOR GRIS	46%
1172167	CONMUTADOR 10 GB ETHERNET CISCO 3650 COLOR GRIS	46%
1180471	SISTEMA DE ALMACENAMIENTO UNITY 450 AFA	50%
1049027	EQUIPO PARA COMUNICACIÓN INALÁMBRICA, BH150 MBPS, CONECTORIZADO 5.7 GHZ LINK	52%
1043949	SWITCH, WS-C2960XR	52%
1043946	SWITCH, WS-C2960XR	52%
1043934	SWITCH, WS-C3650-48PD	52%
1043935	SWITCH, WS-C3650-48PD	52%

1043952	ROUTER ASR-1004	52%
1043953	ROUTER ASR-1004	52%
1043936	SWITCH, WS-C3650-48PD	52%
1043933	SWITCH, WS-C3650-48PD	52%
1043950	SWITCH, WS-C4500X-16	52%
1043951	SWITCH, WS-C4500X-16	52%
1043947	SWITCH, WS-C2960XR	52%
1043948	SWITCH, WS-C2960XR	52%
1260488	SERVIDOR DELL POWEREDGE R730	52%
1260487	SERVIDOR DELL POWEREDGE R730	52%
1260486	DATA DOMAIN (EQUIPO DE RESPALDOS DELL)	52%
1260484	SAN SWTICHES BROCADE	52%
1260485	SAN SWTICHES BROCADE	52%
1064963	EQUIPO PARA LA PREVENCION DE INTRUSOS EN LA RED, DEL TIPO APPLIANCE PARA INSTALARSE EN RACK DE DOS U, METALICOS	53%
1064961	EQUIPO PARA PREVENCION DE INTRUSIONES DE RED Y ANTIMALWARE COLOR ROJO TIPO APLIANCE.	53%
1064962	EQUIPO PARA PREVENCION DE INTRUSIONES DE RED Y ANTIMALWARE COLOR ROJO TIPO APLIANCE.	53%
1064964	EQUIPO PARA PREVENCION DE INTRUSIONES DE RED Y ANTIMALWARE COLOR ROJO TIPO APLIANCE.	53%
1064965	SERVIDOR DE ALTA COMPLEJIDAD PARA EL ANALISIS DE PROTOCOLOS DE SEGURIDAD COLOR NEGRO CON PLATEADO	53%
1064966	SERVIDOR DE ALTA COMPLEJIDAD PARA EL ANALISIS DE PROTOCOLOS DE SEGURIDAD COLOR NEGRO CON PLATEADO	53%
1064970	MURO DE FUEGO PARA PROTECCION DE DATOS EN LA RED TIPO APLIANCE COLOR ROJO	53%
1064969	MURO DE FUEGO PARA PROTECCION DE DATOS EN LA RED TIPO APLIANCE COLOR ROJO	53%
1064967	MURO DE FUEGO PARA PROTECCION DE DATOS EN LA RED TIPO APLIANCE COLOR ROJO	53%
1064968	MURO DE FUEGO PARA PROTECCION DE DATOS EN LA RED TIPO APLIANCE COLOR ROJO	53%
1204401	EQUIPO ADMINISTRACIÓN AVAMAR M600 GEN4T (DATOS ADICIONALES: APM00180623209, APM00180623208 Y APM00180623209).	58%
1204402	EQUIPO DE RESPALDOS DATA DOMAIN (DATO ADICIONAL: APM00181120906).	58%
1204404	SISTEMA DE ALMACENAMIENTO MODELO V5030	59%
1209552	SERVIDOR 8404 MODEL 44E	59%
1204403	SISTEMA DE ALMACENAMIENTO FLASHSYTEM MODELO V9000 (DATO ADICIONAL 78CH081)	59%
1209551	SERVIDOR 8404 MODEL 44E	59%
1189624	CISCO FIREPOWER 2140 NGFW APPLIANCE 1U, 1 X NETMOD BAY	60%
1189621	CISCO FIREPOWER 2140 NGFW APPLIANCE, 1U, 1 X NETMOD BAY	60%
1189622	CISCO FIREPOWER 2140 NGFW APPLIANCE, 1U, 1 X NETMOD BAY	60%
1189623	CISCO FIREPOWER 2140 NGFW APPLIANCE, 1U, 1 X NETMOD BAY	60%
1117046	EQUIPO MCAFEE ENTERPRISE SECURITY MANAGER (MFE ENT SEC MGR, ELMAND EVTREC 5600 APP.	63%
1117047	EQUIPO LOG MANAGER (MFE ENT LOG MGR 4600 APPL)	63%
1117048	EQUIPO EVENT RECEIVER (MFE EVENT RECEIVER 1260 APPL).	63%
1233326	ORACLE SPARC S7-2; MODEL FAMILY	64%

1233327	ORACLE SPARC S7-2; MODEL FAMILY	64%
1242024	EQUIPO MCAFEE WEB GATEWAY MODELO 5500 APPL-D	66%
1242023	EQUIPO MCAFEE WEB GATEWAY MODELO 5500 APPL-D	66%
1233345	GABINETE METÁLICO NEGRO 42RU	66%
1233340	GABINETE METÁLICO NEGRO 42RU	66%
1233339	GABINETE METÁLICO NEGRO 42RU	66%
1233338	GABINETE METÁLICO NEGRO 42RU	66%
1233337	GABINETE METÁLICO NEGRO 42RU	66%
1233336	GABINETE METÁLICO NEGRO 42RU	66%
1233335	GABINETE METÁLICO NEGRO 42RU	66%
1233334	GABINETE METÁLICO NEGRO 42RU	66%
1233333	GABINETE METÁLICO NEGRO 42RU	66%
1233332	GABINETE METÁLICO NEGRO 42RU	66%
1233331	GABINETE METÁLICO NEGRO 42RU	66%
1233330	GABINETE METÁLICO NEGRO 42RU	66%
1233329	GABINETE METÁLICO NEGRO 42RU	66%
1233341	GABINETE METÁLICO NEGRO 42RU	66%
1233342	GABINETE METÁLICO NEGRO 42RU	66%
1233343	GABINETE METÁLICO NEGRO 42RU	66%
1233344	GABINETE METÁLICO NEGRO 42RU	66%
1148541	SISTEMA DE BALANCEO DE CARGAS BASADOS EN IP	69%
1148542	SISTEMA DE BALANCEO DE CARGAS BASADOS EN IP	69%
1008600	SERVIDOR DE VIDEOCONFERENCIA SEGUN CARACTERISTICAS PARA SEGURIDAD DE CONEXIONES EXTERNAS (VCS EXPRESSWAY)	72%
1256933	SERVIDOR IBM 8408 MODELO 44E CON SOFTWARE	74%
1256934	EQUIPO FLASH SYSTEM V9000 STORAGE CON 28.8 TB UTILIZABLES . TRABAJA CON ISCSI Y CON FIBRA CANAL SAN .	74%
1260512	SERVIDOR POWEREDGE R730	78%
1260513	SERVIDOR POWEREDGE R730	78%
1260515	SAN SWITCH CORE DEL DATACENTER	79%
1260516	SAN SWITCH CORE DEL DATACENTER	79%
986984	SISTEMA DE DETECCIÓN Y SUPRESIÓN DE INCENDIOS.	80%
1264867	PUNTO DE ACCESO INALAMBRICO CISCO 1852 COLOR BLANCO CON ANTENAS, TIPO A	82%
1264866	PUNTO DE ACCESO INALAMBRICO CISCO 1852 COLOR BLANCO CON ANTENAS, TIPO A	82%
1233348	UPS SISTEMA DE POTENCIA INTERRU. EMRSON LIEBERT EXM 47SA040	83%
1233347	AIRE ACONDICIONARIO EMERSON LIEBERT CRV CR020RA1C7H319	83%
1233346	AIRE ACONDICIONARIO EMERSON LIEBERT CRV CR020RA1C7H319	83%
1233350	UPS UNIDAD SISTEMA ININTERRUMPIDA EMERSON LIEBERT EXM 47SA100	83%
1233349	UPS UNIDAD SISTEMA ININTERRUMPIDA EMERSON LIEBERT EXM 47SA100	83%
1260522	SERVIDOR HP DL380 GEN9	85%

Fuente: Consulta efectuada al Sistema Contable de Bienes Muebles (SCBM).