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

ATIC-0016-2025
9 de mayo de 2025

RESUMEN EJECUTIVO

El presente estudio fue realizado de acuerdo con el Plan Anual Operativo 2025 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión de Servicios, Configuración, Normativa y Seguridad de Cómputo en la nube a nivel institucional.

Los resultados del estudio permitieron evidenciar que la Caja Costarricense de Seguro Social (CCSS) dispone de una “Hoja de Ruta Estrategia de Habilitación y Migración de Servicios en la Nube”, la cual, si bien representa un avance importante, presenta oportunidades de mejora. Su fortalecimiento o, en su defecto, la formulación de un plan de acción detallado, permitirían no solo asegurar la continuidad y calidad de los servicios institucionales, sino también optimizar el uso de los recursos disponibles, bajo un enfoque de sostenibilidad y disponibilidad que respalde las decisiones asociadas a la ruta tecnológica definida.

Sin embargo, se constató que la cartera de proyectos incluida en la mencionada estrategia no se encuentra registrada en la Agenda Digital Institucional (AGEDI) ni en el Banco de Iniciativas Estratégicas, a pesar de haber sido planteada para ejecutarse en el período 2024-2028.

Desde esta perspectiva, se identificó la ausencia de un marco regulatorio que respalde de manera efectiva la implementación y adopción de servicios tecnológicos en la nube; situación que representa una oportunidad de mejora para establecer, de forma integral, coordinada y completa, el conjunto de normas, políticas, procedimientos y controles necesarios para la contratación, operación, protección, auditoría y supervisión de estos servicios.

En relación con la metodología utilizada para la determinación de necesidades vinculadas a los servicios en la nube, se detectaron debilidades relacionadas con una estimación poco específica y una limitada participación de los Centros de Gestión Informática (CGI) de la institución ; afectando la precisión en la identificación de las necesidades institucionales y, en consecuencia, la priorización adecuada de las mismas, aspecto que resulta fundamental para planificar las eventuales contrataciones administrativas requeridas.

En cuanto a la gestión actual de los servicios en la nube, se observaron debilidades, tanto operativas, como administrativas, entre ellas: limitaciones en la capacidad técnica del recurso humano, falta de articulación entre áreas, dependencia de personal clave, restricciones contractuales, ausencia de monitoreo proactivo, velocidad para la adopción de buenas prácticas, así como deficiencias en seguridad y estandarización; elementos que comprometen la sostenibilidad, eficiencia y evolución de la plataforma, generando la necesidad de fortalecer los mecanismos de gobernanza, planificación, gestión de riesgos y capacidades técnicas institucionales.

Asimismo, no se evidenció la existencia de programas de capacitación estructurados y de amplio alcance relacionados con los servicios en la nube. Las acciones formativas identificadas se han concentrado en el personal de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), sin alcanzar niveles de efectividad ni cobertura adecuados hacia el resto de las unidades institucionales.

Por último, se evidenciaron oportunidades de mejora en los riesgos identificados por la Dirección de Tecnologías de Información y Comunicaciones, en relación con los factores que pueden incidir en el cumplimiento de los objetivos institucionales, dentro del entorno que rodea la administración de los servicios en la nube. Lo anterior, con el propósito de facilitar la toma de decisiones informadas y la implementación integral de medidas de mitigación eficaces.

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

En virtud de lo expuesto, este Órgano de Fiscalización ha solicitado a la Direccion de Tecnologías de Información y Comunicaciones se adopten acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable y así coadyuvar en el fortalecimiento de las estrategias, alineamiento de las TI y el uso adecuado de los recursos institucionales; bajo principios de eficiencia, eficacia y cumplimiento del ordenamiento jurídico-técnico.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

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

ATIC-0016-2025
9 de mayo de 2025

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DE SERVICIOS, CONFIGURACIÓN, NORMATIVA Y SEGURIDAD DE CÓMPUTO EN LA NUBE A NIVEL INSTITUCIONAL

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo 2025 para el Área de Auditoría de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión de Servicios, Configuración, Normativa y Seguridad de Cómputo en la nube a nivel institucional.

OBJETIVOS ESPECÍFICOS

- Analizar las estrategias, iniciativas y proyectos vinculados a servicios en la nube, considerando su planificación, alcance, objetivos, funcionalidades y nivel de alineación con las necesidades institucionales y buenas prácticas del sector.

- Identificar las normativas y estándares aplicables en la CCSS para los entornos en la nube.

- Revisar los criterios técnicos y administrativos que regulan la asignación y reasignación de servicios de la nube de Microsoft Azure.

- Evaluar las capacidades actuales de la plataforma en la nube, así como del equipo responsable de su administración, verificando su idoneidad técnica, competencias, alineación con buenas prácticas, y cumplimiento de los requisitos operativos necesarios para una gestión eficiente y segura de los servicios.

- Revisar y fortalecer el proceso de identificación de riesgos realizado por la Administración Activa en lo referente a la gestión de la infraestructura en la nube, asegurando un enfoque integral, actualizado y alineado con las particularidades de esta tecnología.

NATURALEZA Y ALCANCE

El estudio comprende la verificación de las acciones efectuadas por la Administración Activa en relación con la gestión de servicios de cómputo en la nube a nivel de la CCSS.

El periodo de evaluación incluye desde el 01 de enero del 2025 al 30 de abril del 2025, ampliándose en los casos donde se consideró necesario.

Lo anterior, de acuerdo con lo dispuesto en las Normas Generales de Auditoría para el Sector Público y Normas para el Ejercicio de la Auditoría Sector Público, divulgadas a través de la Resolución R-DC-064-2014 de la

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Contraloría General de la República, publicadas en La Gaceta 184 del 25 de setiembre 2014, vigentes a partir del 1º de enero 2015 y demás normativa aplicable.

LIMITACIONES

Esta Auditoría mediante oficio AI-0424-2025, del 6 de marzo de 2025, solicitó a los Centros de Gestión Informática (CGI) gerenciales, información sobre la implementación de servicios en la nube para propósitos específicos, como almacenamiento, cómputo o bases de datos, entre otros, que no estén vinculados al contrato vigente de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), sin embargo, a la fecha de conclusión de la aplicación de los procedimientos que sustentan este estudio, no se recibió respuesta de los CGI de la Gerencia de logística y la Gerencia de Pensiones respectivamente, según consta en el Sistema Integrado de Gestión de Auditoría (SIGA) al 30 de abril del 2025.

METODOLOGÍA

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Análisis de la información suministrada por la Dirección de Tecnologías de Información y Comunicaciones (DTIC) vía correo electrónico y oficios en formato digital, sobre las acciones asociadas a la implementación de los servicios de nube en la CCSS.

- Solicitud de información y análisis de documentación aportada por los Centros de Gestión Informática Gerenciales.

- Verificación de la Agenda Digital Estratégica Institucional (AGEDI) correspondiente al III Trimestre del 2024 emitidos por la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

- Revisión del Banco de Iniciativas Estratégicas (BIE), con corte al 14 de abril del 2025, remitido por la Dirección de Planificación Institucional.

- Aplicación de entrevistas y/o sesiones de trabajo con:

  - ✓ Lic. Geiner Gamboa Otárola, Jefe Subárea Gestión de Producción y Administrador del Contrato No. 2024LY-000005-0001101161 “Servicios de Azure Vía Enterprise Agreement"
  - ✓ Licda. Vanessa Carvajal Carmona, Jefe Área de Soporte Técnico, Dirección de Tecnologías de Información y Comunicaciones.
  - ✓ Lic. Erick Vindas Umaña, jefe de la Subárea Seguridad TI, Área de Seguridad y Calidad Informática, Dirección de Tecnologías de Información y Comunicaciones.
  - ✓ Luis Adolfo Andino Quirós, Analista en Sistemas de la Subarea de Soporte a Usuarios, Dirección de Tecnologías de Información y Comunicaciones.

- Encuestas:

  - ✓ Se aplicó una encuesta a través de Microsoft Forms con el objetivo de obtener información sobre la experiencia en el proceso de migración y uso de servicios tecnológicos en la nube. Estos servicios incluyen aplicaciones o sistemas transaccionales, bases de datos, almacenamiento de archivos o respaldos, servicios web/APIs, máquinas virtuales (VMs) y servicios de desarrollo/pruebas (Dev/Test), con el fin de apoyar las necesidades de unidades externas a la Dirección de Tecnologías de Información y Comunicaciones (DTIC). La muestra fue aleatoria e incluyó a usuarios de los sistemas: Sistema Integrado de Pensiones (SIP), Sistema Integrado de Gestión de Auditoría (SIGA), Sistema Integrado de Gestión de Personas Trabajadoras CCSS (SIPE), Sistema de Proyecciones y Valuaciones Actuariales (PROVALACT), Sistema de Información y Evaluación de Riesgo (SIER), Sistema de Información del

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

Área de Estadística en Salud (SIAES) y el Sistema de Archivo y Correspondencia (SAYC). En total, se recibieron 6 respuestas a la encuesta.

En cuando al periodo de aplicación, se llevó a cabo durante el periodo comprendido entre el 29 de abril del 2025 y el 02 de mayo del 2025.

MARCO NORMATIVO

- Ley General de Control Interno, No. 8292, julio 2002.
- Normas de Control Interno para el Sector Público de la Contraloría General de la República, febrero 2009.
- Normas Generales de Auditoría para el Sector Público, Resolución R-DC-064-2014, setiembre 2014.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
- Directriz No. 46-H-MICITT “Las instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura”.
- Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, octubre 2012.
- Directriz para la gobernanza de TIC GG-DTIC-EDM01-IT002, setiembre 2020.
- Modelo Organización de los Centros de Gestión Informática, octubre 2013.

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, 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

Conceptos y definiciones

La tecnología en la nube[1] (conocida en inglés como cloud computing) representa una evolución significativa en la provisión de recursos informáticos y servicios a través de internet, eliminando la necesidad de depender exclusivamente de infraestructura local.

Esto permite a las organizaciones acceder a una amplia gama de servicios de manera flexible y escalable, adaptándose rápidamente a las necesidades cambiantes del mercado. A continuación, se presenta una imagen que resume su concepto y características:

[1] La nube (computación en la nube) es un modelo de prestación de servicios de tecnología que permite acceder a recursos informáticos (como almacenamiento, servidores, bases de datos y software) a través de internet, en lugar de utilizar infraestructura física local. Este modelo ofrece escalabilidad, flexibilidad y costos optimizados, permitiendo a las empresas y usuarios consumir recursos bajo demanda sin necesidad de gestionar directamente la infraestructura subyacente.

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

Imagen No. 1
Concepto y características de la tecnología en Nube

Fuente: Elaboración propia, a partir de la información contenida en https://edteam-media.s3.amazonaws.com/blogs/original/def59e91-b472-40dd-b9c4-cda7f79a3515.png

A ese respecto, las organizaciones pueden utilizar Infraestructura como Servicio (IaaS) para alquilar servidores virtuales y otros recursos, eliminando la necesidad de mantener hardware físico.

Particularmente, la nube se utiliza ampliamente para el almacenamiento de datos, permitiendo a las organizaciones guardar grandes volúmenes de información de manera segura y accesible desde cualquier lugar. Además, es fundamental para la copia de seguridad y recuperación ante desastres, afirmando la protección y recuperación rápida de datos en caso de fallos.

En el ámbito del desarrollo y pruebas de software, la nube ofrece entornos eficientes para crear, probar y desplegar aplicaciones. Por ejemplo, al disponer de una Plataforma como Servicio (PaaS), se proporciona un entorno de desarrollo completo en la nube, permitiendo a los desarrolladores centrarse en la creación de aplicaciones sin preocuparse por la gestión de la infraestructura. Asimismo, el Software como Servicio (SaaS) permite a las organizaciones utilizar aplicaciones basadas en la nube a través de internet, sin necesidad de instalar y mantener software en dispositivos locales.

En el ámbito de las herramientas de colaboración y productividad basadas en la nube, uno de los ejemplos más reconocidos es Microsoft Office 365, que proporciona a los usuarios un entorno sincronizado para trabajar en tiempo real desde cualquier tipo de dispositivo.

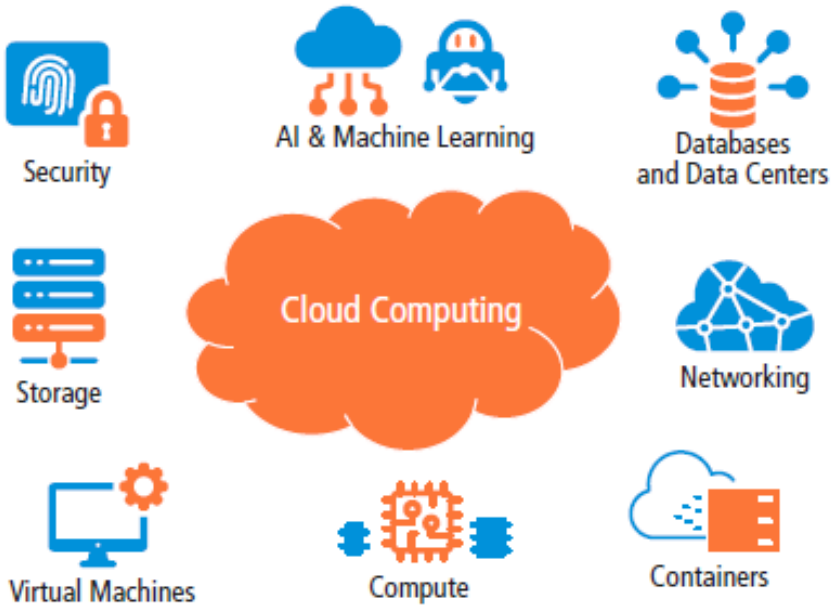
Por otra parte, esta tecnología emergente también facilita el análisis de datos y Big Data[2], proporcionando la infraestructura necesaria para procesar y analizar grandes volúmenes de datos. En el campo de la inteligencia

[2] Big Data es el manejo de grandes volúmenes de datos variados y generados a alta velocidad, que requieren tecnologías avanzadas para su procesamiento y análisis. Se utiliza para obtener información valiosa en la toma de decisiones y optimización de procesos.

artificial[3] y el aprendizaje automático[4], la nube ofrece plataformas y herramientas para desarrollar y desplegar modelos avanzados.

Es decir, la nube funciona como una generalización para referirse a la externalización de datos, aplicaciones o infraestructura, tal y como se observa en la siguiente imagen.

Imagen No. 2
Tipos de datos, aplicaciones y/o infraestructura en la Nube



Fuente: Publicación "Auditoría Interna de la gestión operativa del Cloud", Enero 2025, Instituto de Auditores Internos

Lo anterior, por mencionar algunos de los múltiples usos y variaciones que pueden darse bajo la misma base tecnológica.

Por otra parte, es relevante mencionar que existen múltiples proveedores de servicios en la nube que ofrecen estas capacidades. Entre los más destacados se encuentran Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud y Oracle Cloud. Cada uno de estos proveedores ofrece una variedad de servicios y herramientas que permiten a las organizaciones elegir la solución que mejor se adapte a sus necesidades específicas.

[3] Inteligencia Artificial (IA) es el campo de la informática que desarrolla sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, la toma de decisiones y el reconocimiento de patrones. Utiliza algoritmos y modelos para simular capacidades cognitivas, mejorando con el tiempo a través de la experiencia.

[4] La tecnología de aprendizaje automático (o machine learning) es un subcampo de la inteligencia artificial que permite a las máquinas aprender de los datos y mejorar su rendimiento con el tiempo sin necesidad de ser programadas explícitamente para realizar tareas específicas. Utiliza algoritmos y modelos matemáticos para identificar patrones en los datos, hacer predicciones o tomar decisiones basadas en experiencias previas.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Contexto Institucional

La Caja Costarricense de Seguro Social (CCSS) no ha sido ajena a la adopción de tecnologías avanzadas; desde 2017, la Institución comenzó a implementar servicios basados en la nube, comenzando con la Licitación Pública No. 2017LN-000003-1150 “Licenciamiento Microsoft”, que contemplaba la renovación y actualización del licenciamiento de software de Microsoft, adquiriéndose licencias de Office 365, marcando así los primeros pasos en la habilitación de ese tipo de servicios.

Posteriormente en el 2020, la Dirección de Tecnologías de Información y Comunicaciones gestionó la contratación del “Servicio de Azure vía Enterprise Agreement”, la cual tuvo las siguientes características:

Cuadro No. 1
Datos de la contratación No. 2020LN-000005-1150
Servicios de Azure vía Enterprise Agreement

No. de Procedimiento:	2020LN-000005-1150
Objeto contractual:	Servicios de Azure vía Enterprise Agreement
No. de contrato:	013-2020
Modalidad de entrega:	Según demanda
Limite presupuestario:	$1.000.000.00[5]

Fuente: Elaboración propia.

A partir de ese momento, la CCSS opera en un entorno de nube híbrida, empleando los tres modelos de consumo: SaaS, PaaS e IaaS mencionados anteriormente. A continuación, se presenta un cuadro con la información sobre el consumo realizado por la CCSS, en relación con el monto pagado y la cantidad de tokens[6] de acceso adquiridos, correspondiente a los períodos 2021 a 2023:

Cuadro No. 2
Resumen de Consumo mensual del 2021-2023
Contratación No. 2020LN-000005-1150

Mes	2021	2022	2023
Total Anual	$789,654.75	$1,070,827.34	$890,595.27
Total de Token	6954.25	9430.45	7843.20

Nota: Valor del Token Histórico $113,55.
Fuente: Estudio para determinar la cantidad de Unidades de Consumo Mínimo de Microsoft Azure, Abril 2024.

En ese sentido, el consumo del servicio responde a implementaciones que se encuentran en operación y forman parte del portal de servicios de la Institución, lo cual da continuidad a servicios implementados principalmente en el Datacenter principal ubicado en CODISA[7], a saber:

[5] Al 20 de febrero de 2025, el tipo de cambio del dólar estadounidense es de aproximadamente 505.60 colones costarricenses por dólar1. Por lo tanto, un millón de dólares americanos equivale a aproximadamente 505,600,000 colones costarricenses.

[6] Los tokens de acceso son un tipo de token de seguridad diseñado para la autorización, concediéndole acceso a recursos específicos en nombre de un usuario autenticado. La información de los tokens de acceso determina si un usuario tiene derecho a acceder a un recurso determinado, similar a las claves que desbloquean puertas específicas en un edificio. Tomado del sitio learn.microsoft.com

[7] **Fuente**: solicitud de contratación (Decisión de inicio) 2024LY-000005-0001101161, Servicios de Azure vía Enterprise Agreement, 23 de abril del 2024, página 1-2.

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

- *Correo electrónico.*
- *Active Directory.*
- *Servicios cognitivos Computer Vision.*
  - *Moderador de contenido.*
  - *Servicios de voz.*
  - *Análisis de texto.*
  - *Traductor.*
- *Exchange.*
- *Herramientas de monitoreo.*
- *Contenedores entre otros.*
- *Balanceadores de carga.*
- *Servicios de Pensiones.*
- *Crecimiento de nuevos proyectos que necesitan infraestructura de forma rápida y económica.*
- *Infraestructure as a Service*
  - *Máquinas virtuales para todo propósito (Exchange, Active Directory, Sharepoint, aplicaciones (Linux Based y Windows Based)*
- *Software as a Service Bases de Datos*
  - *Hosted applications/apps (Contenedores)*
  - *Herramientas de desarrollo, administración de datos, análisis de datos.*
- *Platform as a Service (Appliances de diversos fabricantes) Filtrado de correo*
  - *Emulación de aplicaciones*
  - *SendGrid*
  - *Dynatrace*

Además, mediante el contrato N.° 013-2020, derivado de la licitación 2020LN-000005-1150, se habilitó nuevos servicios de Data Center en la nube brindando a la institución la capacidad de implementar servicios de infraestructura y otras soluciones tecnológicas[8]. Entre las principales, se destacan las siguientes:

- *Filtrado de correo Electrónico (Barracuda).*
- *Servicios de Infraestructura de Active Directory y DNS.*
- *Servicio Azure Active Directory.*
- *Servicio de envió masivo de correos SMTP, usando el servicio SendGrid.*
- *El SICERE utiliza un Bot para apoyar tramites y servicios al usuario.*
- *Servidores Exchange ON-PREMISE, se están instalando en la Azure.*
- *La herramienta de monitoreo de aplicaciones corre 100% en nube (Dynatrace).*
- *Para algunos servicios se utilizan balanceadores de carga*
- *Aplicaciones por medio de SaaS*
- *Server de multisesión para RDWeb*
- *Aplicación AGEDI*
- *Indicadores BI*
- *Bot de Company Comunicator*
- *Aplicaciones del HCG.*

La plataforma en la nube continúo en expansión; para el año 2024 se contemplaba la posibilidad de aplicar una prórroga contractual a la licitación No. 2020LN-000005-1150. No obstante, la Administración decidió no ejecutarla, fundamentando su decisión en las limitaciones asociadas al crecimiento del servicio y al tope presupuestario establecido en un millón de dólares, los cuales representaban restricciones para mantener las condiciones contractuales vigentes en ese momento.

De este modo, la Dirección de Tecnologías de Información y Comunicaciones llevó a cabo la contratación N.° 2024LY-000005-0001101161 'Servicios de Azure vía Enterprise Agreement', la cual contempló la continuidad del servicio ya migrado a la nube, así como futuras necesidades considerando que la infraestructura actual no es estática, sino que continúa en expansión y consumiendo recursos. A continuación, se incluye cuadro con información detallada de ese proceso de compra:

[8] **Fuente**: solicitud de contratación (Decisión de inicio) 2024LY-000005-0001101161, Servicios de Azure vía Enterprise Agreement, 23 de abril del 2024, pagina 3.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Cuadro No. 3
Datos de la contratación 2024LY-000005-0001101161
Servicio de suscripción a servicios en nube AZURE de Microsoft

No. de Procedimiento:	2024LY-000005-0001101161
Objeto contractual	Servicio de suscripción a servicios en nube AZURE de Microsoft
Modalidad de entrega	Según demanda
Contratista:	GBM de Costa Rica Sociedad Anónima
Limite presupuestario	$1.600.000.00
Encargado del contrato	Lic. Geiner Gamboa Otárola, jefe Subárea Gestión de Producción, DTIC

Fuente: elaboración propia a partir de lo consultado en SICOP en relación con la contratación No. 2024LY-000005-0001101161.

Bajo esa perspectiva, la Caja ha estado utilizando la tecnología de Microsoft Azure, integrando además servicios como Sengrid, Dynatrace y Barracuda, así como herramientas de seguridad de diversas casas comerciales, lo que ha resultado en un consumo significativo. Esto se debe tanto a los recursos que ofrece la plataforma en la nube como a la integración de ambientes tecnológicos, lo cual propicia el desarrollo y alojamiento de sistemas y aplicaciones que están actualmente habilitados en la Nube[9]:

- *Agente Virtual SICERE (ChatBot)*
- *Express Route*
- *Servicio Dashboard Covid HRCG*
- *Infraestructura_CCSS_RGE*
- *Servicio Network Watcher*
- *Servicio de Active Directory*
- *Servicio VDI SGP*
- *Grupo de recursos Azure Back Up*
- *Serv. Monitoreo Dynatrace*
- *Servicio Azure ARC (Servidores OnPremise)*
- *Revisión por demanda de productos MS*
- *Recursos Assesment Migración*
- *SDP para servidores AD*
- *Servicio de Filtrado Correo Barracuda*
- *Servicio de Presupuesto (SGBD)*
- *Service Communicator (mensajes globales)*
- *Serv. de bóveda de respaldos AD*
- *Servicio Microfilmación (DSI)*
- *Servicio de Check Point*
- *Servicio Control de acceso*
- *Servicio Diabetes Mellitus-EDUS*
- *Servicio DevOps (Desarrollo aplicaciones)*
- *Servicio de correo Exchange*
- *Servicio Gerencia Pensiones (Aplicación lógica)*
- *Registro de acciones de los administradores*
- *Servicio LimeSurvey (Epidemiología)*
- *Logs Analytics*
- *Servicio Migración Cuentas Correo*
- *Servicio Appliance Migración HGC*
- *Log Analytics SP a SPO*
- *Log Analytic Patch Reports interno*
- *Servicios Licencias Power Designer*
- *Servicio VDI Active Directory (Mesa Servicios)*
- *Servicios Web REDATAM*
- *Servicio Web SIPE (RRHH)*
- *Registro de Logs de Sing-ins (Seguridad TI)*
- *Servicio SICORE (DSI)*
- *Servicio SIEM (Seguridad TI)*
- *Servicio SIER (Actuarial)*
- *Servicio Web SIGA (Auditoría Interna)*
- *Servicio Web SIGES en línea*
- *Servicio SMTP Correo Sendgrid*
- *Nube M-365*

En este contexto, la implementación de servicios en la nube por parte de la CCSS se materializó a través de los contratos supracitados, sin embargo, al carecer de una estrategia clara y alineamiento a una gobernanza que impulsara un proceso estructurado y masivo para la adopción de la solución, se dificultó la identificación y priorización integral de las necesidades. Ante ello, en 2024, se elaboró una "Hoja de Ruta Estrategia de Habilitación y Migración de Servicios en Nube", en seguimiento a lo acordado en Junta Directiva en el artículo 132 de la sesión N° 9189, celebrada el 24 de junio de 2021, que cita textualmente:

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

[9] **Fuente**: Minuta 01-2025 del 04 de abril de 2025, correspondiente a la sesión del Consejo Tecnológico Institucional.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

De este modo, el documento fue recibido por el Consejo Tecnológico el 4 de abril de 2025, según consta en la sesión No. 01-2025 de dicho órgano[10], mediante el acuerdo primero relacionado con el tema de Nube, en el cual se cita lo siguiente:

> *"Dar por recibido la Estrategia de Habilitación de Servicios en Nube de la Dirección de Tecnologías de Información y Comunicaciones como parte de un sitio alterno y adopción tecnológica para garantizar la continuidad de las operaciones TIC, y en atención a los diferentes Informes de Auditoría, Consejo Tecnológico y Acuerdos de Junta Directiva."*

A partir de esa presentación, se establece una visión general de las actividades desarrolladas e implementadas como parte de la Hoja de Ruta para la migración de los servicios TIC del Centro de Datos en Tierra hacia Centros de Datos en la Nube durante el período 2024-2028.

En este contexto, la hoja de ruta supracitada contempla el desarrollo de cuatro proyectos clave, orientados a los siguientes objetivos:

- Tecnologías x86 y Bases de Datos SQL: Identificar servicios en tecnologías x86 (Microsoft Windows), que son candidatos para migrar de su estado actual en premisa (Tierra), a un Centro de Datos en Nube (Microsoft Azure).
- Tecnología Unix y Oracle: Investigar las alternativas de equipos de misión crítica de alta disponibilidad y escalable bajo demanda en la Nube, que le permita a la Caja Costarricense de Seguro Social migrar y ejecutar las cargas de procesamiento, almacenamiento y su crecimiento, para las capas de base de datos y aplicaciones del servicio institucional SICERE, así como otros servicios integrados, consolidando los ambientes productivos y no productivos.
- Conectividad Segura: Habilitar de manera segura e independiente, la conectividad de los sitios CCSS, aprovechando las nuevas tecnologías bajo el estándar SASE (SD-WAN + SSE).
- Monitoreo como servicio: Adquirir un servicio 24x7x365 para el monitoreo, análisis, supervisión y administración de los eventos de la plataforma tecnológica institucional, que garantice la disponibilidad de servicios tecnológicos a la población interna y externa, detectando alertas, canalizando al personal técnico encargado y el seguimiento de la alerta para mitigar sus efectos. A su vez fortalecer e implementar el modelo de gobernanza con procesos ya documentados que permitan mejorar la gestión en TIC en la institución acorde a lo establecido en el Sistema de Gestión de Servicios de la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

Así mismo, en la sesión supracitada se indicó que la Hoja de Ruta no puede ser implementada sin un adecuado dimensionamiento de los costos; en ese sentido, la ejecución de la estrategia, incluyendo todos los proyectos mencionados anteriormente, contempla una inversión estimada de $15,854,378.62 (quince millones ochocientos cincuenta y cuatro mil trescientos setenta y ocho dólares con sesenta y dos centavos) para el período 2025-2028.

Por tanto, las etapas subsiguientes consistirán en poner en marcha la ejecución de la estrategia mediante los mecanismos de control establecidos en el propio documento y proyectados a largo plazo. Asimismo, se deberá dar cumplimiento al acuerdo segundo, relacionado con el tema de nube, aprobado en esa misma sesión, en el cual se solicitó:

> *"Instruir a Dirección de Tecnologías de Información y Comunicaciones para que continúe con la implementación de la Hoja de Ruta propuesta en la estrategia en la que se determinen actividades, plazos, responsables y la viabilidad financiera. La Dirección de Tecnologías de Información y Comunicaciones deberá presentar avances trimestrales al Consejo Tecnológico."*

[10] Acta en condición de borrador, pendiente de formalización mediante recolección de firmas, con fecha de corte al 2 de mayo de 2025.

Productos de Auditoría relacionados a la temática

Sobre el particular, este Órgano Fiscalizador ha emitido informes y documentos relacionados con la implementación y adopción de la nube, entre los cuales se destacan:

Cuadro No. 4
Productos emitidos por la Auditoría en Tecnologías de Información y Comunicaciones sobre la tecnología de Nube

NO. INFORME	FECHA	ASUNTO
ATIC-166-2020	11 de diciembre de 2020	El informe sobre la Plataforma Tecnológica Central revela la falta de una estrategia integral, deficiencias en continuidad operativa, planificación de capacidad, renovación de activos, pruebas de continuidad, rendición de cuentas e indicadores. También alerta sobre la dependencia de proveedores, afectando inversiones superiores a $15 millones y la toma de decisiones estratégicas.
AS-ATIC-674-2021	24 de marzo de 2021	Oficio de asesoría preventiva sobre preparación tecnológica de la CCSS, señalando temas clave como teletrabajo, ciberseguridad, inteligencia artificial, nube, telemedicina, capacitación virtual, hiperautomatización, 5G, internet del comportamiento, automatización financiera e Industria 4.0, para anticipar desafíos y oportunidades.
AS-AATIC-177-2022	23 de agosto de 2022	El informe responde a los ciberataques de 2022 que afectaron la infraestructura tecnológica de la CCSS, recomendando evaluar la computación en la nube como alternativa de contingencia. Detalla tipos y modelos de nube, destacando beneficios operativos y normativos para fortalecer la continuidad y ciberseguridad institucional.
ATIC-0080-2024	11 de diciembre del 2024	El estudio señala la falta de una hoja de ruta y marco regulatorio para tecnologías emergentes como la computación en la nube. Destaca la necesidad de dirección estratégica clara y formación continua del personal, para garantizar una gestión adecuada y alineada con la evolución tecnológica en la CCSS.

Fuente: elaboración propia, Auditoría Interna.

HALLAZGOS

1. SOBRE LA CARTERA DE PROYECTOS INDICADOS EN LA "HOJA DE RUTA ESTRATEGIA DE HABILITACIÓN Y MIGRACIÓN DE SERVICIOS EN NUBE"

Se evidenció que la cartera de proyectos contemplada en la "Hoja de Ruta Estrategia de Habilitación y Migración de Servicios en la Nube" no ha sido incorporada en el Banco de Iniciativas[11] ni en el Portafolio de Proyectos TIC, conocido como la Agenda Digital Institucional (AGEDI)[12], según lo estipulado en la Directriz para la Gobernanza de TIC y el Manual de Procedimientos del Banco de iniciativas y Portafolio de Proyectos Institucional.

Esta omisión resulta preocupante, especialmente considerando la complejidad del mismo y los elementos involucrados, entre los que se incluyen: la inversión de recursos económicos para habilitar infraestructura y tecnología; los períodos de ejecución (establecidos entre 2024 y 2028) e incluso el impacto a la operativa en cuanto a la asignación de equipos de trabajo dedicados; la aplicación de metodologías para la gestión de proyectos; el análisis de regulaciones y normativas; la capacitación y transferencia de conocimiento; la gestión del cambio organizacional; la identificación, tratamiento de riesgos y contingencias; la participación de las partes interesadas; la definición de indicadores y métricas de seguimiento; entre otros elementos.

[11] Mecanismo de control "Iniciativas BIE" con corte al 14 de abril de 2025, en el cual no se registra ninguna iniciativa relacionada con Tecnologías de Información y Comunicaciones (TIC).
[12] Según consulta efectuada a la Subárea Administración de Proyectos de la DTIC el último informe de AGEDI es el correspondiente al tercer trimestre del 2024, según consta en correo remitido el 11 de marzo del 2025.

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002, en su apartado 7.3 establece que:

> *"7.3 Toda iniciativa relacionada con la entrega de servicios de TIC deberá alinearse al Plan Estratégico Institucional vigente.*
>
> *El uso de las tecnologías de información posibilitará y entregará valor estratégico al negocio. La orientación tecnológica de la CCSS debe responder a una visión de negocio, de manera que se asegure el alineamiento de las inversiones y la congruencia entre la evolución de la plataforma y los servicios de negocio. Para la presentación de propuestas de una iniciativa de carácter tecnológico o con componentes tecnológicos significativos, se desarrollará un caso de negocio que ayude a conocer el esfuerzo que representa la iniciativa, alcance, objetivos preliminares, así como beneficio y valor esperado a partir de la iniciativa, y su respectiva vinculación con las estrategias institucionales.".*

El Manual de Procedimientos del Banco de Iniciativas y Portafolio de Proyectos Institucional (2020) establece las directrices para la recepción de estudios de preinversión, la priorización estratégica de proyectos y la integración formal del portafolio institucional.

> *"Para el caso de los proyectos con componente TIC deberán ser incluidos dentro de la AGEDI (Agenda Digital Institucional), que en este documento es equivalente al Subportafolio TIC. El responsable de gestionar la AGEDI es la Dirección de Tecnologías de Información y Comunicación".*

Por otra parte, el Manual de la Agenda Digital Estratégica Institucional (SAP-MAN-001-2022), en el punto 5 "Agenda Digital Estratégica Institucional" indica:

> *"La AGEDI registra información clave de los programas y* ***proyectos para facilitar la toma de decisiones y el seguimiento****, cuya fuente de información se encuentra en los documentos, reportes y mecanismos que se han definido como el medio de retroalimentación y estado de los proyectos. Así, por ejemplo, en la AGEDI se incluye una referencia o resumen de los riesgos de un programa o proyecto, mientras que la identificación y la valoración de riesgos y las estrategias para su gestión estarán en los casos de negocio u otros documentos de seguimiento y gestión.*
>
> *Por otra parte, la AGEDI permite la generación de información necesaria* ***para apoyar el análisis y gestión de portafolio****; por ejemplo, elementos para identificar los impactos esperados en los servicios TIC o en el modelo operativo institucional.*
>
> *Con esta información, el Consejo Tecnológico dispone de elementos* ***para apoyar sus actividades, consultar o convocar a involucrados clave*** *para programas, proyectos o temas específicos y respaldar la toma de decisiones que permitan a la Institución reducir riesgos y aumentar el valor del portafolio de proyectos con componentes tecnológicos".* ***El resaltado no pertenece al original.***

La Licda. Vanessa Carvajal Carmona, Jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, se refirió a la inclusión de los proyectos en los diferentes sistemas de AGEDI, manifestando lo siguiente:

> *"Las iniciativas no están registradas en AGEDI porque estamos trabajando bajo una estrategia de carácter general y global. Algunas iniciativas, como la renovación de la plataforma tecnológica, sí se encuentran en AGEDI, ya que forman parte del fondo de inversión del presupuesto, el cual exige ese registro formal.*
>
> *Sin embargo, estas iniciativas no están registradas porque se ejecutan bajo el presupuesto ordinario y no requieren estar vinculadas a AGEDI, así nos lo explicaron.*

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Por esta razón, algunas acciones de la estrategia están reflejadas en AGEDI, mientras que otras no, dependiendo de su fuente de financiamiento."

Además, la Licda. Vanessa Carvajal Carmona señaló las medidas adoptadas para evitar afectaciones en los proyectos que, conforme a la "Hoja de Ruta de la Estrategia de Habilitación y Migración de Servicios en la Nube", debían iniciar en el año 2024, indicando lo siguiente:

"Respecto a las iniciativas de 2024, te comento que ya las teníamos planificadas y hemos venido trabajando en ellas, pese a no haber estado aprobada la estrategia en ese momento. En ese sentido, el tener aprobación de la estrategia viene a garantizarnos el financiamiento necesario (ampliación de presupuesto), recordemos que los recursos ya existían, pero estaban proyectados para ser distribuidos en determinados proyectos y en un plazo de cuatro años.

En otras palabras, los avances que hemos logrado se pudieron asumir sin necesidad de la estrategia; sin embargo, la restricción presupuestaria al aprobarse la estrategia debería quedar superada, ya que se acordó ante el Consejo Tecnológico ir trabajando en línea con lo necesario para materializar el conjunto de proyectos."

Pese a lo señalado como causa de la situación detectada, esta Auditoría considera que, dada la relevancia estratégica de la "Hoja de Ruta Estrategia de Habilitación y Migración de Servicios en la Nube", así como la magnitud de recursos involucrados y la exposición al riesgo derivada del nivel de madurez institucional en la adopción de soluciones en la nube, resulta fundamental que esta iniciativa sea gestionada desde su inicio bajo un enfoque de proyecto formal. Esta gestión permitiría establecer mecanismos adecuados de control, seguimiento y rendición de cuentas. En ese sentido, los subproyectos derivados, así como las unidades programáticas involucradas, deberían ser estructurados también como proyectos específicos y no abordarse únicamente como labores operativas, ya que esta última modalidad no garantiza un nivel suficiente de compromiso, ni asegura el cumplimiento de los objetivos estratégicos planteados.

De no oficializarse ni comunicarse oportunamente los proyectos y/o iniciativas, existe el riesgo de que no se materialice o que presente deficiencias significativas en su planificación, supervisión y alineación estratégica, comprometiendo su implementación efectiva y limitando su aporte a los objetivos institucionales.

Adicionalmente, podrían gestionarse como actividades operativas iniciativas que, por su complejidad e impacto, deberían tratarse como proyectos formales, aspecto que agravaría la falta de control y seguimiento estructurado, reduciendo la efectividad de los resultados esperados, en detrimento del uso racional de los recursos institucionales.

2. SOBRE LA INICIATIVA DE HABILITACIÓN Y MIGRACIÓN DE SERVICIOS EN LA NUBE

Se identificaron oportunidades de mejora en el diseño de la documentación asociada a la "Hoja de Ruta Estrategia de Habilitación y Migración de Servicios en la Nube" elaborada por la Dirección de Tecnologías de Información y Comunicaciones, la cual incluye tanto la visión general y/o el enfoque a largo plazo; como consideraciones preliminares sobre tiempos, recursos y responsables que podrían dar forma a un futuro plan de acción.

En ese sentido, el conjunto de proyectos incluidos en la estrategia puede fortalecerse mediante una mejor definición de los datos y elementos contextuales que sustentan cada uno de los objetivos propuestos. Esto resulta especialmente relevante considerando que diversos grupos de interés requerirán dicha información para su correcta interpretación y aplicación.

A partir de lo anterior, se identifican los siguientes factores que requieren mayor atención, a saber:

- **Evaluación de las condiciones actuales de los servicios de nube (previo al nuevo despliegue):** La estrategia actual parte de una planificación operativa enfocada en la migración de componentes sin que se

evidencie una evaluación institucional integral que identifique las capacidades actuales y las brechas a nivel organizativo, normativo, de competencias y de procesos que podrían condicionar el éxito del despliegue.

La ausencia de este diagnóstico y recomendaciones imposibilita anticipar ajustes necesarios antes de una expansión mayor de los servicios en la nube.

- **Integración del grupo de interesados:** La estrategia no evidencia si el componente de negocio ha sido adecuadamente involucrado (de manera preliminar) o si ha habido una socialización clara de los objetivos y la necesidad de esta iniciativa desde el punto de vista tecnológico; lo cual compromete la posibilidad de impulsar una gobernanza efectiva y alineada con los objetivos institucionales.

  En ese sentido, los actores del negocio son fundamentales en este proceso, ya que son los principales usuarios (solicitantes de los servicios) y responsables funcionales de sistemas críticos como el EDUS (considerando el conjunto de aplicativos), SICERE, ERP, plataformas de Business Intelligence (BI), entre otros aplicativos igualmente esenciales.

  La omisión de su participación desde las etapas iniciales de la estrategia limita una comprensión realista de las capacidades de adopción de servicios en la nube. Además, retrasa o dificulta la planificación de actividades clave como la reingeniería de aplicaciones, la gestión de la seguridad de la información, la clasificación de datos y la gestión del cambio organizacional. Esta falta de previsión pone en riesgo la adopción exitosa del proyecto y podría generar resistencias internas o problemas operativos significativos ya estando aprobada la estrategia y habiéndose aumentado el presupuesto que respalda dicha implementación.

  Como ejemplo, en el oficio GM-CGI-0058-2025 / HSJD-CGI-084-2025 / DRIPSSHA-CGI-0011-2025 / HMACE-DAF-CGI-0016-2025, del 24 de marzo de 2025, suscrito por el M.Sc. Esteban Zúñiga Chacón, jefatura del Centro de Gestión Informática de la Gerencia Médica; el Ing. Dagoberto Camacho Aguilar, en representación de Hospitales Nacionales; la Ing. Kricia Valverde Rodríguez, representante de Direcciones Regionales; y el Ing. David Mora Mora, representante de Hospitales Especializados (todos(as) ellos(as), jefaturas de distintos Centros de Gestión Informática) se manifiesta la necesidad de contar con una estrategia institucional claramente definida y debidamente socializada.

  En dicho documento, se indica lo siguiente:

  > *"Es nuestro criterio que, igualmente, se establezca la estrategia institucional recomendada, se socialice con las instancias que corresponda y se opte por la mejor de estas. De manera tal que se logren objetivos comentados como: alta disponibilidad, bajos costos, facilidad para los usuarios y agilidad para el personal TIC; pero además se consideren aspectos de seguridad de la información, confidencialidad de los datos, leyes y normativas aplicables a la CCSS (aplicativos en salud), ley de protección de datos de las personas y afines."*

- **Gestión de riesgos a nivel estratégico:** dada la mención de riesgos que se hace en la estrategia para determinados entornos y las pretensiones de abordarlos mediante la adopción de servicios en la nube; es de vital importancia especificar de manera integral cuáles riesgos podría enfrentar los proyectos y cómo gestionarlos desde el nivel estratégico.

  En este contexto, la falta de un apartado específico que detalle los riesgos asociados a la estrategia, especialmente en la fase de planificación, dificulta asegurar su viabilidad, particularmente dada su alta complejidad y consecuentemente la solidez de esta.

Ahora bien, el pasado 4 de abril de 2025, el Consejo Tecnológico Institucional recibió formalmente la Estrategia de Habilitación de Servicios en la Nube, según consta en el acta de la sesión No. 01-2025. En esa misma sesión, dicho Órgano instó a continuar con su implementación, estableciendo como siguiente paso la definición de actividades, plazos, responsables y la evaluación de la viabilidad financiera.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

En coherencia con esta solicitud, es fundamental que los proyectos incluidos en la estrategia cuenten con los insumos requeridos por el Consejo, así como con documentación complementaria que permita una mayor comprensión y claridad, facilite la priorización adecuada y contribuya a un dimensionamiento preciso de las tareas a ejecutar.

Por otra parte, y considerando los aspectos previamente señalados, la estrategia establece una vinculación preliminar con un posible plan de acción. Si bien esto no constituye una debilidad en sí misma, se considera necesario profundizar en varios de los componentes incluidos, con el fin de fortalecer su operatividad y direccionar su implementación, a saber:

- **Actividades por desarrollar y su medición:** Aunque se incluye un cronograma de actividades, este carece de los detalles generales necesarios para facilitar la comprensión de las labores a realizar y sus responsables, ya que algunas iniciativas solo indican que se extenderán por un período de tres años, lo cual resulta impreciso.

  Además, existen ejemplos de actividades cuya comprensión podría verse afectada por la falta de una descripción detallada, como es el caso de las actividades 8 (BI), 12 (Nuance), 13 (Gestión Documental), 14 (Otros) y 16 (X); incluso escueta en determinados casos.

- **Criterios de éxito:** Aunque la estrategia menciona "criterios de éxito necesarios" vinculadas a las actividades por desarrollar, no se definen cuáles serán las métricas específicas y medibles para cada una de ellas, lo que dificulta la evaluación precisa del término utilizado.

- **Gestión de múltiples proveedores de nube (Multi-Cloud):** Aunque el documento hace referencia a los distintos tipos de computación en la nube (pública, privada e híbrida), no aborda aspectos críticos como la interoperabilidad entre plataformas, la gestión de contratos con múltiples proveedores, la portabilidad de las cargas de trabajo, ni la necesidad de una gobernanza unificada. Estos elementos son fundamentales para una implementación efectiva en entornos multi-nube y deben ser desarrollados con mayor profundidad para contar con los insumos que orienten al grupo de involucrado en la toma de decisiones correspondientes al mediano y largo plazo, garantizando la sostenibilidad y escalabilidad de la estrategia.

  Incluso en el documento se habla del criterio actual para la selección de tecnologías de servicios en la nube, que se centra en Microsoft Azure al considerarse una “alternativa segura” debido a contratos previamente establecidos. Sin embargo, es fundamental ampliar esta visión para incorporar un análisis integral del abanico de opciones disponibles, considerando la dinámica cambiante del mercado, el plazo requerido para la implementación en los distintos sitios de la CCSS y la evaluación de la viabilidad técnica y económica de cada alternativa. Esta perspectiva permitiría una toma de decisiones más estratégica, informada y sostenible en el tiempo.

En síntesis, las observaciones planteadas corresponden principalmente al nivel estratégico y apuntan a mejorar la claridad y solidez de su formulación. Considerar estos elementos resultara clave, ya que la estrategia y documentación de apoyo serán objeto de análisis, y su aplicación dependerá de la consistencia de los componentes supracitados.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado “I. Gobierno de TI”, cita:

> *“La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.*
>
> *La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las*

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales.

La conceptualización de este órgano rector debe ser una instancia de alto nivel que busca habilitar la gobernanza en torno a las Tecnologías de la Información y Comunicaciones (TIC), estableciendo un espacio de diálogo y coordinación entre las gerencias de la institución y la unidad responsable de las Tecnologías de Información y Comunicaciones (DTIC), con el fin de asegurar el apoyo de las TIC a la gestión y el cumplimiento de la estrategia institucional. Al estar integrado por las máximas autoridades de gobierno y administración de la Institución, junto con la unidad de Tecnologías de la Información y Comunicaciones, y la Direccion de Planificación Institucional asume como cuerpo colegiado, la toma de decisiones sobre temas estratégicos asociados con las TIC que inciden en la prestación de los servicios a los usuarios."

Además, ese mismo marco normativo en su apartado III. Planificación Tecnológica Institucional señala:

"La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público.

Adicionalmente, que incorpore indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia. (…)

Finalmente, esas Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT, en el apartado XIV. Aseguramiento, indica lo siguiente:

"(…) La institución debe estar comprometida en la aplicación de buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el cumplimiento de regulaciones internas y externas, así como disposiciones contractuales. (…)"

Las Normas Institucionales en TIC, en el apartado 1.1. Marco estratégico de TIC, menciona que:

"(…)1.1.2 La Dirección de Tecnologías de Información y Comunicaciones es la responsable de formular, actualizar y administrar las políticas, normas, estándares, guías y procedimientos Institucionales en materia de tecnologías de información y comunicaciones.

1.1.3 La Dirección de Tecnologías de Información y Comunicaciones construye y somete a aprobación de las autoridades competentes las políticas, estrategias, normas, estándares y procedimientos, que regulen el accionar de las TIC en la Institución. Así mismo, debe promover y divulgar este marco regulatorio. (…)"

Esas mismas normas institucionales, en el apartado 2.1 Planificación de las tecnologías de información, inciso 2.1.5 señalan que:

"A la Dirección de Tecnologías de Información y Comunicaciones le corresponde administrar el desarrollo óptimo de la transferencia, adaptación y funcionamiento de las tecnologías de información y comunicaciones; y establecer la regulación, la normativa técnica y la coordinación en el nivel institucional que guíe y oriente el desarrollo de las tecnologías de información y comunicaciones.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Asimismo, ejercer autoridad funcional y técnica en materia de tecnologías de información y comunicaciones en el ámbito institucional."

La Licda. Vanessa Carvajal Carmona, Jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, se refirió al diseño de la estrategia indicando lo siguiente:

"*Respecto a la claridad del alcance, la estrategia está diseñada para aplicarse a nivel institucional. Cada proyecto contempla la incorporación paulatina de las diferentes necesidades que puedan surgir en las unidades. Si existiera algún aspecto que generara confusión, este sería atribuible únicamente a temas de redacción.*

En cuanto a los demás factores que podrían representar oportunidades de mejora en la definición de la estrategia, no se desarrollan a detalle porque se tiene claro que dentro de cada uno de los cuatro proyectos incluidos en la hoja de ruta deberán especificar posteriormente las actividades convenientes a cada caso. De hecho, ya se debe ir trabajando en ellos, siguiendo la línea de que cada proyecto cuente con su propio nivel de detalle, incluyendo la definición de actividades, responsables, plazos y entregables."

La ausencia de consideraciones en la estrategia de cómputo en la nube tales como: las mencionadas anteriormente puede generar vacíos y confusión que afecten las etapas posteriores de ejecución; cuando elementos como actividades, riesgos, involucramiento del componente de negocio, documentación de apoyo, entre otros no están claramente definidos, se dificulta la coordinación, el cumplimiento de plazos y el aprovechamiento adecuado de los recursos, aumentando el riesgo de desviaciones en los proyectos y comprometiendo su alineación con los objetivos institucionales

3. SOBRE LA DISPONIBILIDAD DE UN MARCO NORMATIVO

Se identificó que, aunque la Caja Costarricense de Seguro Social implementó servicios de computación en la nube a través de la plataforma Microsoft Azure desde el año 2020, aún no dispone de un marco regulatorio que establezca, de manera integral, coordinada y completa, el conjunto de normas, políticas, procedimientos y controles necesarios para la contratación, operación, protección, auditoría y supervisión de los servicios en la nube.

Bajo este contexto, no se identifica documentación que respalde adecuadamente la gestión táctica y operativa de los entornos en la nube, lo que dificulta, entre otros aspectos, la definición precisa de roles y responsabilidades, tanto a nivel interno (áreas técnicas y del componente de negocio) como externo (proveedores y socios tecnológicos). Esta situación genera ambigüedad entre las distintas áreas funcionales respecto a las tareas que deben ejecutarse y a la asignación de responsabilidades en la operación de los servicios en la nube. Además, la documentación existente como manuales de puestos, manuales de organización y normas TIC, sigue enfocada en el modelo de infraestructura física y no ha sido actualizada para reflejar las exigencias del nuevo entorno tecnológico.

Por otra parte, entre la documentación aportada por la Administración Activa se identificó el documento titulado "GG-DTIC-GCSN-IT004 Procedimiento de Catálogo de Servicios en la Nube v 1.0", junto con plantillas asociadas[13], los cuales abordan solo un componente específico dentro de la gestión de servicios en la nube. Ahora bien, pese a indicarse que están oficializados, los documentos se encuentran en formato editable, carecen de firmas y no están publicados en la intranet institucional, específicamente en el sitio web de la DTIC, dentro del apartado "Normativa TIC y Procedimientos TIC", bajo la categoría correspondiente a "Procedimientos", según se verificó al 24 de abril de 2025, aspectos que deben ser revisados y corregidos por esa Administración Activa.

[13] GG-DTIC-GCSN-IT005 Especificación de Propuesta Servicios en la nube v 1.0; GG-DTIC-GCSN-IT006 Desestimación de propuesta de servicio en la nube v 1.0; GG-DTIC-GCSN-IT007 Coordinación cronograma para valoración de servicio en la nube v 1.0; GG-DTIC-GCSN-IT008 Cronograma de Trabajo para la valoración de servicio en la nube v 1.0; GG-DTIC-GCSN-IT009 Informe y criterio de valoración de servicio en la nube v 1.0; GG-DTIC-GCSN-IT010 Servicio preparado para implementación en la nube v 1.0.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT, en el apartado XIV. Aseguramiento, indica lo siguiente:

> *"(…) La institución debe estar comprometida en la aplicación de buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el cumplimiento de regulaciones internas y externas, así como disposiciones contractuales. (…)"*

Las Normas Institucionales en TIC, en el apartado 1.1. Marco estratégico de TIC, menciona que:

> *"(…)1.1.2 La Dirección de Tecnologías de Información y Comunicaciones es la responsable de formular, actualizar y administrar las políticas, normas, estándares, guías y procedimientos Institucionales en materia de tecnologías de información y comunicaciones.*
>
> *1.1.3 La Dirección de Tecnologías de Información y Comunicaciones construye y somete a aprobación de las autoridades competentes las políticas, estrategias, normas, estándares y procedimientos, que regulen el accionar de las TIC en la Institución. Así mismo, debe promover y divulgar este marco regulatorio. (…)"*

Esas mismas normas institucionales, en el apartado 2.1 Planificación de las tecnologías de información, inciso 2.1.5 señalan que:

> *"A la Dirección de Tecnologías de Información y Comunicaciones le corresponde administrar el desarrollo óptimo de la transferencia, adaptación y funcionamiento de las tecnologías de información y comunicaciones; y establecer la regulación, la normativa técnica y la coordinación en el nivel institucional que guíe y oriente el desarrollo de las tecnologías de información y comunicaciones.*
> *Asimismo, ejercer autoridad funcional y técnica en materia de tecnologías de información y comunicaciones en el ámbito institucional."*

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002 en el apartado 7.5 y 7.5.1, menciona lo siguiente:

> *"**7.5 La DTIC es responsable de la emisión de normativa interna como ente rector en materia tecnológica**.*
>
> *La normativa interna relativa a la gestión y gobernanza de las TIC a nivel institucional es responsabilidad de la DTIC, por lo que es competencia exclusiva de esta unidad organizacional emitir, revisar, aprobar, actualizar y divulgar toda aquella documentación enfocada en dirigir el desarrollo de las actividades relacionadas con la puesta en marcha de los procesos TIC, en línea con lo definido en el Manual para la generación y administración de normativa y documentación de soporte a los procesos, servicios y operaciones de TIC así como con el modelo de toma de decisiones, respectivamente.*
>
> *Dicha documentación es de acatamiento obligatorio por todas y cada una de las partes involucradas, lo cual alcanza a personal de las áreas de negocio, específicamente en materia de gobernanza y gestión de TIC.*
>
> ***7.5.1 Mecanismo***
> *Se llevará a cabo una revisión y actualización periódica de la base documental normativa y de apoyo a la gestión de los procesos TIC, conforme lo establecido en el Manual para la generación y administración de normativa y documentación de soporte a los procesos, servicios y operaciones de TIC."*

En el oficio GG-DTIC-1939-2025 27 de marzo de 2025 suscrito por el Máster Robert Picado Mora, director de la Dirección de Tecnologías de Información y Comunicaciones, se refiere a la ausencia de marco normativo, citando:

> *"Este marco normativo, se estará realizando en lo solicitado en la recomendación 2 del Informe ATIC-0080-2024 dirigido al Consejo Tecnológico referente a "Auditoría de carácter especial sobre la gestión de las*

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

tecnologías emergentes en la CCSS" y en donde se solicita la elaboración del marco normativo que regule a nivel institucional la gestión de las tecnologías emergentes en la Institución."

El Lic. Erick Vindas Umaña, jefe de la Subárea de Seguridad TI de la Direccion de Tecnologías de Información y Comunicaciones, al referirse a la ausencia de un marco regulatorio y de documentación interrelacionada, señaló:

"(…) es fundamental que se definan claramente los roles y las responsabilidades, de modo que el equipo de ciberseguridad pueda enfocarse en su función sin verse sobrecargado. Esto implica no solo la definición de perfiles de puesto, sino también la creación o actualización de manuales organizacionales, directrices y políticas, entre otros documentos clave, los cuales, en la actualidad, no existen o no han sido actualizados para reflejar nuestra nueva realidad.

(…) No puedo dejar de mencionar que, lamentablemente, la tendencia actual es que cualquier asunto relacionado con seguridad termine siendo asignado a nuestro equipo, aunque en muchos casos no nos corresponde directamente. Es necesario establecer mecanismos claros que nos permitan defender nuestra posición, ya que actualmente se nos están endosando procesos que, en rigor, no deberían ser gestionados exclusivamente por nosotros. Esto genera una carga operativa que limita nuestra capacidad de intervenir de manera efectiva en operaciones que realmente requieren atención especializada.

Debemos aspirar a tener una capacidad resolutiva real, con roles claramente definidos, para abordar únicamente aquellas operaciones que nos competen. No podemos seguir funcionando bajo un esquema en el que simplemente se asignan responsabilidades por salir del paso."

Sobre ese mismo tema, la Licda. Vanessa Carvajal Carmona, jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, indicó:

"Al comparar toda la documentación que hemos desarrollado para la gestión de la infraestructura física — la cual incorporaba un conjunto robusto de mejores prácticas, procedimientos estandarizados, lineamientos técnicos y criterios de configuración, no contamos con un equivalente para el entorno de nube

(…) Actualmente vemos una necesidad urgente de que se defina de forma clara y formal una directriz interna en la institución que establezca la importancia estratégica de estos proyectos, y que obligue a las demás áreas de trabajo a apoyar de manera efectiva. No puede ser opcional ni depender de voluntades individuales.

Otro tema crítico es la definición de roles y responsabilidades. Actualmente, en el entorno de nube, no está claramente establecido quién debe asumir qué funciones. En infraestructura física esto sí estaba definido, pero en nube aún existe mucha confusión. Esta falta de definición genera problemas reales: responsabilidades que nadie asume formalmente y situaciones de riesgo que quedan sin atender."

Además, la Licda. Vanessa Carvajal Carmona, jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, se refirió al procedimiento "GG-DTIC-GCSN-IT004 v 1,0" y las plantillas asociadas, citando:

"El procedimiento del catálogo de servicios y las plantillas asociadas ya están oficializados. Este proceso es gestionado por Danilo Hernández, quien coordina la recepción y el primer filtro de las solicitudes.

Cuando una unidad requiere algún servicio, el primer paso es completar un formulario de solicitud. Esta solicitud llega a Danilo, quien realiza una revisión inicial (registro) y, a partir de ahí, inicia la validación de aspectos como costos, viabilidad técnica y prioridades, por parte del equipo correspondiente.

En su momento, Danilo trabajó en la estandarización de este proceso, elaborando formularios estructurados que permiten registrar los datos y validaciones a medida que avanza cada proyecto. Es

importante señalar que este procedimiento no se gestiona a través de un sistema de software específico, sino que se organiza mediante dashboards de control, donde se realizan el seguimiento de los proyectos."

La ausencia de un marco normativo específico para la computación en la nube en la Caja Costarricense de Seguro Social genera un entorno de incertidumbre que limita la dirección, coordinación y control sobre su adopción, implementación y gestión operativa. Esta carencia dificulta la toma de decisiones estratégicas, la asignación clara de responsabilidades y la aplicación uniforme de criterios técnicos, legales y de seguridad. Como resultado, se incrementan los riesgos en áreas críticas, comprometiendo la eficiencia, sostenibilidad y continuidad de los servicios tecnológicos, con un impacto directo en la gobernanza de la nube, la seguridad de la información, la protección de datos y propiedad intelectual, el cumplimiento normativo, la gestión de incidentes y la contratación, administración y supervisión de estos servicios.

4. SOBRE LA DETERMINACIÓN DE NECESIDADES PARA ADQUIRIR SERVICIOS DE NUBE EN MICROSOFT AZURE

Se identificaron oportunidades de mejora en la estimación efectuada y metodología utilizada para determinar las necesidades institucionales de adquisición y/o consumo en los recursos de nube proporcionados por Microsoft Azure.

Lo anterior, se fundamenta en la revisión del proceso utilizado en la compra N° 2024LY-000005-0001101161 Servicios de Azure Vía Enterprise Agreement", concretamente en el documento "Estudio para determinar la cantidad de Unidades de Consumo Mínimo de Microsoft Azure" de abril del 2024, realizado por el Lic. Geiner Gamboa Otárola, jefe de la Subárea de Gestión de Producción, y encargado general del contrato Servicios de Azure Vía Enterprise Agreement. A continuación, se detallan las debilidades observadas:

- No se presenta un análisis integral y detallado de toda la plataforma tecnológica de la Institución que relacione la operación de la infraestructura física con las necesidades futuras de incorporación a los servicios en la nube (migración a infraestructuras lógicas) en el corto, mediano y largo plazo.

- No se establece una priorización de las soluciones institucionales que deberían considerarse en el uso y aprovechamiento de la contratación.

- El documento se limita a referenciar el consumo histórico (2021-2023), a partir del cual se proyecta una tendencia de consumo. En cuanto a las estimaciones relacionadas con soluciones específicas, se hacen sin justificar su selección ni relevancia en relación con otras posibles necesidades.

- La estimación de crecimiento de iniciativas específicas se limita a citar sus nombres, sin detallar los recursos tecnológicos requeridos (almacenamiento lógico) para cada solución.

- No se evidencia en el documento la participación de los Centros de Gestión Informática gerenciales, regionales o locales. El estudio fue desarrollado y coordinado exclusivamente por funcionarios del Área de Soporte Técnico de la Direccion de Tecnologías de Información y Comunicaciones, específicamente por el Ing. Esteban González Monge, jefe de la Subárea Base de Datos; la Bach. Angie Melissa Chacón Chavarría, Operador de Plataforma Tecnológica; y el Lic. Geiner Gamboa Otárola, Encargado General del Contrato Microsoft Azure.

A partir de lo anterior, es criterio de esta Auditoría que el estudio realizado durante esa contratación podía haberse apoyado de mayores elementos de análisis que permitieran identificar y estimar las necesidades lo más certeramente posible en materia de consumo proyectado; lo anterior, se comprueba en la falta articulación entre la DTIC, CGI e involucrados a nivel de negocio; aspecto que resulta indispensable para determinar los recursos necesarios en el nivel central, regional y local, por tanto, las oportunidades de mejora se encuentran orientadas a disponer de metodologías o procesos sistemáticos orientados a garantizar de forma razonable que las inversiones realizadas en estas tecnologías responden a criterios técnicos definidos integralmente con la

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

participación de todos o al menos una representación razonable de los diferentes actores que intervienen en la gestión TIC de la CCSS.

Las Normas Institucionales TIC, en el apartado 1.1 Marco Estratégico, inciso 1.1.4, señala que:

> *"Los Centros de Gestión Informática participan en la formulación, actualización y la evaluación de la regulación, la normativa técnica, proponiendo los protocolos y los estándares de calidad, con el propósito de lograr uniformidad en los proyectos de TIC y la maximización de los recursos institucionales. "*

Esas mismas Normas, en el apartado 2.1 Planificación de las tecnologías de información, inciso 2.1.5 señalan que:

> *"A la Dirección de Tecnologías de Información y Comunicaciones le corresponde administrar el desarrollo óptimo de la transferencia, adaptación y funcionamiento de las tecnologías de información y comunicaciones; y establecer la regulación, la normativa técnica y la coordinación en el nivel institucional que guíe y oriente el desarrollo de las tecnologías de información y comunicaciones.*
>
> *Asimismo, ejercer autoridad funcional y técnica en materia de tecnologías de información y comunicaciones en el ámbito institucional."*

Además, ese mismo marco normativo en el inciso 2.1.6 cita:

> *"Los Centros de Gestión de Informática (CGI) son responsables de impulsar e implementar en forma efectiva las soluciones en tecnologías de información y comunicaciones en el ámbito gerencial, regional y local, con base en las necesidades de los usuarios, de la organización y las posibilidades financieras de la Institución, según se establece en el documento Modelos de Organización de los Centros de Gestión Informática."*
>
> *El Manual de Organización de la Dirección de Tecnologías de Información (2013), señala dentro de las actividades sustantivas del Nivel Dirección, Gestión Estratégica lo siguiente:*
>
> *"(…) Asesorar y coordinar actividades con los Centros de Gestión Informática, a partir de los requerimientos de la organización, la regulación y la normativa vigente, con el propósito de lograr el desarrollo efectivo de la gestión y la participación de estas unidades de trabajo. (…)"*

El Modelo de Organización de los CGI, menciona en el apartado 5.4 5 Conceptualización del Centro de Gestión Informática, lo siguiente:

> *"(…) Es responsable de realizar las actividades operativas que apoyan el desarrollo de las tecnologías de información y comunicaciones, la ejecución de estudios de necesidades, la automatización de procesos estratégicos y operativos, participa activamente en la elaboración de planes, la administración de proyectos el desarrollo de los sistemas automatizados, implementa los mecanismos de coordinación, de comunicación, aplica las nuevas tecnologías, administra los equipos y las redes de información en su ámbito de competencia; es un enlace entre los usuarios no especializados, la Dirección de Tecnologías de Información y Comunicaciones y otros órganos competentes.*
>
> *Los Centros de Gestión Informática son responsables del desarrollo operativo y la coordinación de actividades, en el nivel gerencial, regional y local.*
>
> *Deben establecer una comunicación e interrelación efectiva con las unidades de trabajo afines, con el Consejo Institucional de Centros de Gestión Informática y con la Dirección de Tecnologías de Información y Comunicaciones, con el fin de mantener la integración y estandarización en el desarrollo e implementación de los sistemas de información y racionalidad en la administración de los recursos. (…)"*

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Ese mismo Modelo, en las funciones sustantivas del CGI Gerencial, gestión técnica, señala:

> *"(…)Coordinar acciones con la Dirección de Tecnologías de Información y Comunicaciones, el Consejo Institucional de Centros de Gestión Informática, los Centros de Gestión Informática regionales, locales y las unidades de trabajo (en su ámbito de competencia), de conformidad con los requerimientos de la organización, con el propósito de lograr la integración y la comunicación de los sistemas de información, el desarrollo de proyectos estratégicos, específicos y efectividad en el desarrollo de la gestión, entre otros aspectos.(…)"*

Lic. Geiner Gamboa Otárola, encargado general del contrato Servicios de Azure Vía Enterprise Agreement, indicó:

> *"El mapeo completo de la infraestructura física existente y con probabilidades de migrar es un tema complejo que requiere un trabajo exhaustivo, incluyendo estudios técnicos, estimaciones de costos y pruebas.*
>
> *La CCSS podría tener fácilmente alrededor de 500 servidores (solo en la plataforma central), lo que implicaría la necesidad de coordinar con diversas áreas para realizar una estimación precisa. Debido a esto, hemos tenido que dosificar la liberación de la herramienta de manera controlada.*
>
> *Además, existen numerosos aplicativos y servidores que incluso se replican en varias unidades programáticas, lo que añade una capa adicional de complejidad al proceso. Un ejemplo que permite dimensionar la magnitud del esfuerzo requerido para estimar e implementar la nube en la institución puede encontrarse en proyectos anteriores como SICERE, EDUS, SIFA, ERP, entre otros.*
>
> *En todos estos casos, la DTIC asumió las labores técnicas necesarias para la ejecución de los proyectos, pero sin que se produjera un ajuste proporcional en la dotación de recursos humanos. Esta desproporción ha derivado en cargas de trabajo operativas difíciles de sostener en el tiempo, lo que obliga al equipo a concentrarse únicamente en las tareas críticas del proceso, sin margen para profundizar en aspectos técnicos, perfeccionar prácticas existentes o fomentar la especialización. Esta situación limita significativamente la posibilidad de implementar mejoras continuas, sin ser la excepción la computación en la nube.*
>
> *Bajo esa misma lógica, la adopción de Azure —y más aún si se considera una estrategia multicloud— podría estar expuesta a un crecimiento desmedido en las responsabilidades técnicas y de gestión, si no se toman las previsiones necesarias desde ahora.*
>
> *Lo ideal sería abordar este proceso de migración por etapas, permitiendo así un crecimiento controlado y manejable. No obstante, es importante tener presente que el identificar todas las posibles necesidades de la CCSS - no solo del nivel central - implica una mayor carga de trabajo en términos de gestión y administración. Soy plenamente consciente de la necesidad de contar con un mapeo completo de la infraestructura, pero también de las limitaciones existentes, particularmente en cuanto a recurso humano. La ausencia de un equipo dedicado exclusivamente a apoyar esta migración hace prácticamente imposible llevar a cabo el proceso de forma masiva, razón por la cual se ha optado por una identificación gradual y progresiva de las necesidades."*

La falta de articulación y metodología integral en la determinación de necesidades para adoptar la computación en la nube en la CCSS podría generar resultados ineficientes y potencialmente imprecisos, afectando la calidad de las estimaciones y dando lugar a posibles sobreestimaciones o subestimaciones en el consumo real requerido en la Institución.

Del mismo modo, la situación descrita comprometería la percepción del proceso de contratación, al interpretarse como una opción de consumo para determinados usuarios únicamente o como una respuesta bajo un enfoque reactivo ante situaciones no previstas.

5. SOBRE LA ADMINISTRACIÓN DEL SERVICIO DE NUBE

Entre los principales hallazgos identificados por esta Auditoría, se constató que la gestión operativa y administrativa de los servicios de computación en la nube en la Caja Costarricense de Seguro Social enfrenta limitaciones que afectan su desempeño y sostenibilidad.

Estas limitaciones, identificadas por el Área de Soporte Técnico, la Subárea de Gestión de Producción y la Subárea de Seguridad TI, todas pertenecientes a la Dirección de Tecnologías de Información y Comunicaciones (DTIC), se relacionan principalmente con la gestión del recurso humano y del conocimiento técnico; la gestión contractual y de infraestructura; el monitoreo, la evaluación y la optimización operativa; así como la gestión de configuración y la aplicación de buenas prácticas en la administración de la nube, a saber:

A. Gestión del recurso humano y conocimiento técnico

- **Capacidad (cantidad) e integración (cohesión) del equipo de trabajo:** Se identificó una percepción, por parte de la Administración Activa, de que los equipos actuales no cuentan con la capacidad suficiente (en términos de cantidad de personal y dedicación exclusiva) para gestionar con la agilidad requerida los entornos en la nube. Sin embargo, no se evidenciaron estudios o análisis técnicos que determinen cuántos recursos humanos serían necesarios para afrontar adecuadamente el cambio hacia una nueva plataforma tecnológica en la nube. Tampoco se pudo establecer si este requerimiento obedece a una necesidad real de incrementar el número de personas o a una necesidad de reconversión de habilidades en el personal ya existente; situación que incrementa las dificultades para asumir eficientemente las tareas de administración, control y apropiación técnica del nuevo entorno tecnológico.

  Además, los jefes de área y subárea de la DTIC entrevistados señalaron oportunidades de mejora en cuanto a la cohesión y el nivel de involucramiento del equipo en la atención de las necesidades asociadas a la gestión de la infraestructura en la nube. Según sus opiniones, aún persisten desafíos en la articulación y colaboración entre los distintos miembros del equipo, lo cual podría estar limitando una respuesta integral y proactiva frente a los requerimientos técnicos y operativos de la transición tecnológica.

  Aunado a lo anterior, esta situación también ha sido percibida por unidades programáticas externas a la DTIC. Al ser consultadas sobre los principales obstáculos o dificultades enfrentadas en los procesos de migración, se señalaron aspectos como la necesidad de coordinar separadamente los temas de seguridad, infraestructura y redes con cada unidad responsable, lo cual retrasa los avances. Asimismo, los funcionarios consultados recomendaron considerar la incorporación de desarrolladores especializados en nube y perfiles DevOps para fortalecer los procesos de migración, así como mejorar la integración con el Area de Ingeniería en Sistemas de la DTIC. Una de las observaciones destacadas sugiere que la DTIC debería conformar un grupo de apoyo interdisciplinario con capacidad de decisión y acción, que acompañe desde el inicio los proyectos de migración, permitiendo una mayor claridad sobre los requerimientos técnicos desde el principio, facilitando una respuesta más ágil y evitando demoras ocasionadas por la falta de elementos clave, como configuraciones de red o seguridad.

- **Falta de gestión de conocimiento técnico:** Según lo indicado por el Administrador del Contrato correspondiente a la licitación No. 2024LY-000005-0001101161 “Servicio de suscripción a servicios en nube AZURE de Microsoft”, la Subárea de Gestión de Producción sigue dependiendo del conocimiento especializado de un funcionario, quien, durante la vigencia del contrato pasado No. 2020LN-000005-1150 “Servicios de Azure vía Enterprise Agreement”, concentró funciones y conocimientos técnicos;

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

dependencia que se originó ante la falta de un enfoque multidisciplinario y a la ausencia de una estrategia estructurada para la gestión y distribución del conocimiento dentro del equipo.

Actualmente, este funcionario se encuentra en la Subárea de Administración de Plataformas, pero sigue brindando colaboración para fortalecer al equipo y transferir conocimiento, lo que subraya la importancia de gestionar el despliegue de esta tecnología de manera ordenada, evitando riesgos como la dependencia de personal específico, que limita la participación de otros involucrados en el proceso. Por lo tanto, lo señalado por la Administración Activa no solo refleja lo ocurrido, sino que también sirve como una advertencia para prevenir que esta situación se repita, incluso con una mayor asignación de recursos en las condiciones actuales.

B. Gestión contractual

- **Carga de trabajo del administrador del contrato:** Según lo indicado por el Administrador del Contrato correspondiente a la licitación No. 2024LY-000005-0001101161 “Servicio de suscripción a servicios en nube AZURE de Microsoft”, su capacidad para liderar y contribuir de manera efectiva se ve limitada por la disponibilidad de tiempo, ya que debe atender múltiples responsabilidades. En ese sentido, comentó:

  “Lamentablemente, no puedo liderar y/o aportar como quisiera debido a que existen otras responsabilidades que requieren mi atención.
  A nivel operativo y/o presupuestario, se podría pensar que se requiere una respuesta más rápida, pero debo dosificar los esfuerzos para mantener un ritmo controlado que permita al equipo sostener la carga de trabajo.

  Además, la administración del contrato se percibe como una carga adicional, especialmente considerando que, hasta el momento, estoy a cargo de cinco contrataciones, lo cual complica aún más las labores diarias. A esto se suma que están en curso nuevas licitaciones, lo que incrementa aún más la carga de trabajo, mientras que en la subárea solo somos seis personas.”

  Asimismo, es importante señalar que el Lic. Geiner Gamboa Otárola ocupa la jefatura de la Subárea de Gestión de Producción en la Dirección de Tecnologías de Información y Comunicaciones, donde lidera un equipo compuesto por solo seis personas.

- **Restricciones del crecimiento en la infraestructura:** El contrato actual presenta limitaciones para escalar la infraestructura, ya que está sujeto a los topes presupuestarios definidos en el marco de la licitación “Servicios de Azure vía Enterprise Agreement”. En la contratación No. 2020LN-000005-1150, el monto anual máximo era de $1.000.000, mientras que en la contratación No. 2024LY-000005-0001101161 dicho tope se incrementó a $1.600.000, lo que representa un aumento del 60 %.

  Sin embargo, el costo estimado para implementar la estrategia de Habilitación de Servicios en la Nube durante un periodo de cuatro años asciende a $15.854.378,62. En ese contexto, las capacidades presupuestarias del contrato vigente resultan insuficientes para atender el creciente volumen de requerimientos asociados con la gestión del servicio en la nube, especialmente tras la reciente aprobación de la estrategia institucional para fortalecer su implementación en la CCSS, situación que compromete la capacidad de respuesta ante el aumento sostenido en la demanda

C. Monitoreo, evaluación y optimización operativa

- **Evaluaciones periódicas sobre optimización de costos y beneficios:** Se identificó la ausencia de evaluaciones periódicas, sistemáticas y profundas orientadas a analizar la eficiencia del gasto asociado a la operación en la nube, así como a valorar los beneficios reales obtenidos desde su adopción en la CCSS. Este tipo de análisis resulta esencial no solo para justificar el uso de recursos públicos, sino también para identificar oportunidades de mejora, eficiencia y ajuste en la estrategia tecnológica.

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

Hasta el momento, el único estudio de costos realizado se centró en una comparación puntual entre el uso de Azure VMware Solution (AVS) en la nube de Microsoft Azure[14] y una alternativa basada en VMware on-premise[15]. Sin embargo, no se han encontrado análisis más amplios que consideren escenarios alternativos, modelos híbridos o proveedores distintos. Tampoco se evidencia una valoración estratégica sobre la elección de Azure como proveedor principal, **ni una evaluación del grado de dependencia tecnológica que dicha elección podría estar generando para la institución a través del tiempo**. Este tipo de consideraciones son clave para asegurar una gestión sostenible, transparente y con márgenes de maniobra técnica y financiera en el futuro.

- **Seguimiento estructurado y proactivo para el control técnico-operativo de la plataforma en la nube:** Se constató que la gestión operativa del entorno en la nube carece de un enfoque proactivo, periódico y estructurado que permita identificar y atender de manera oportuna vulnerabilidades, oportunidades de mejora y acciones para optimizar el rendimiento de la plataforma. Si bien existen herramientas como reportes de uso y consumo del portal de Azure, métricas de desempeño generadas por servicios de monitoreo (como Azure Monitor o Log Analytics), el Administrador de Contrato de la licitación No. 2024LY-000005-0001101161 indica que sería de mayor utilidad informes elaborados por el proveedor en el marco del contrato vigente.

  Es decir, si bien el portal de Azure proporciona herramientas básicas (dashboards para el monitoreo del uso de recursos, costos y comportamiento general), resulta necesario avanzar hacia esquemas de monitoreo personalizados que permitan un control más eficiente y adaptado a las necesidades específicas de la institución. No obstante, según lo señalado por la Administración, el diseño e implementación de estas soluciones requeriría una asignación presupuestaria adicional, así como una considerable dedicación de tiempo y esfuerzo por parte del equipo técnico, recursos que actualmente no se encuentran disponibles.

  Adicionalmente, no existe un proceso formal y continuo de escaneo mediante herramientas especializadas del equipo de seguridad, que permita generar informes periódicos sobre configuraciones inseguras, brechas técnicas o servicios mal implementados; Lo cual la misma Administración ha identificado como una oportunidad de mejora que debe documentar e incluso incorporar como parte de las iniciativas que van a ser desarrolladas en el Plan de Ciberseguridad en TIC institucional.

D. Gestión de configuración y buenas prácticas de administración de la nube

- **Estrategia de segmentación de red:** La Administración Activa ha señalado la falta de una implementación oportuna de mecanismos de segmentación de red, como la microsegmentación. Esta omisión compromete la capacidad de contener incidentes de seguridad, aumenta el riesgo de propagación lateral de amenazas, expone servicios críticos y reduce la eficacia de la respuesta ante posibles brechas. La adopción de estas medidas no debe posponerse a fases avanzadas del proceso de migración, ya que su implementación temprana es esencial para fortalecer el modelo de seguridad desde su fase de diseño.

- **Controles de seguridad previos a la publicación de aplicaciones en la nube:** actualmente no se cuenta con un proceso establecido y formalizado para la evaluación de seguridad de aplicaciones de software (sistemas de información) previa al paso a producción. En consecuencia, aplicativos desplegados en ambientes productivos no son sometidos a validaciones exhaustivas ni a pruebas de vulnerabilidades, deficiencia que incrementa el riesgo de exposición a amenazas y pone en riesgo la integridad del entorno.

- **Ritmo en la adopción de buenas prácticas:** Según lo esbozado por el Administrador de Contrato de la licitación No. 2024LY-000005-0001101161 se han dedicado esfuerzos por incorporar buenas prácticas, en

[14] Azure VMware Solution (AVS) permite ejecutar cargas de trabajo de VMware directamente en la infraestructura de Azure, sin necesidad de rediseñarlas.
[15] Es la implementación de entornos virtualizados VMware dentro del propio centro de datos físico de la organización (infraestructura local).

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

acompañamiento con Microsoft, pero el avance ha sido limitado. La falta de capacidad de los equipos ha impedido aplicar mejoras de manera oportuna y con la prioridad que requieren la infraestructura cloud, lo que compromete la madurez de la operación y eleva el riesgo de que se consoliden brechas técnicas. Si bien recientemente se ha avanzado en la implementación de landing zones, como parte de las buenas prácticas recomendadas para una gestión estructurada y segura de la nube, estos esfuerzos aún son aislados y requieren mayor continuidad. Esta situación evidencia la necesidad de fortalecer la estructura organizativa y técnica para acelerar la adopción de mejores prácticas y garantizar una gestión más eficaz y sostenible de la plataforma.

- **Estandarización en la nomenclatura en el nombre y/o grupo de los recursos en Azure**: se identificó que algunos recursos creados en la plataforma de Azure como máquinas virtuales y cuentas de almacenamiento no siguen los prefijos de nomenclatura estándar. Esta falta de uniformidad dificulta la gestión eficiente de los recursos, incrementa el riesgo de errores en operaciones administrativas, complica las auditorías técnicas y obstaculiza la automatización de tareas y la integración de nuevas herramientas.

  Para ejemplificar lo indicado anteriormente, se citan a continuación casos identificados en el documento titulado “3.d. Inventario de recursos Azure - 14-03-2025”, adjunto al oficio GG-DTIC-2281-2025 del 10 de abril de 2025, suscrito por la Licda. Vanessa Carvajal Carmona, Jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones:

Cuadro No. 5
Identificación de Oportunidades de Mejora en la Nomenclatura de Recursos en Azure

Detalle / Descripción	Tipo de recurso	Falta de estandarización	
		Nombre	Grupo de recurso
DeasarrolloPruebas	Azure Virtual Machine	X	
Temporalborrar	Azure Virtual Machine	X	
gpenccss	Azure Virtual Machine		X
infraestructura_ccss_rge	Azure Virtual Machine		X
cs710033fff9bd0b9bf	Azure Storage Accounts	X	
7s5bk37n2zcg2	Azure Storage Accounts	X	
infraestructura_ccss_rge	Azure Storage Accounts		X
cloud-shell-storage-southcentralus	Azure Storage Accounts		X

Fuente: “3.d. Inventario de recursos Azure - 14-03-2025”, adjunto al oficio GG-DTIC-2281-2025 del 10 de abril de 2025

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT, en el apartado VII. Recursos Humanos, señala:

> *“La Unidad de TI debe constituirse con funcionarios que dispongan de un perfil técnico de acuerdo con sus responsabilidades, así como habilidades de gestión y administrativas que permitan realizar actividades requeridas para asegurar la gobernanza de las TI.”*

Esas mismas Normas en su apartado VIII. Contratación y Adquisiciones de Bienes y Servicios Tecnológicos, señala que:

> *“La Unidad de TI debe disponer y aplicar en forma consistente prácticas para la supervisión y evaluación a través de pruebas de aceptación y valoración del cumplimiento contractual en cuanto al servicio y desempeño en la implementación, configuración y administración de los recursos tecnológicos contratados a terceros.”*

Del mismo modo, en el apartado XI. Seguridad y Ciberseguridad, cita que:

"La institución debe implementar medidas de control asociadas a la administración del riesgo de seguridad de la información y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información."

Además, esa misma norma del MICITT en el apartado XII. Administración Infraestructura Tecnológica, indica lo siguiente:

"La Unidad de TI debe establecer prácticas formales para la gestión de la entrega de servicios a través de los recursos tecnológicos instalados en la institución, administrados interna y externamente, gestionando la configuración y mantenimiento del desempeño y capacidad de los activos de TI, de manera que a través de monitoreos y actualizaciones se mantenga el uso óptimo de los recursos y brinden una garantía razonable sobre la continuidad de las operaciones institucionales, establecidos a través de niveles de operación y sostenibilidad para brindar los servicios requeridos."

Finalmente, en el apartado XIV. Aseguramiento, señala que:

"La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados. Adicionalmente, debe asegurar que las unidades institucionales disponen y aplican prácticas e instrumentos que le permitan evaluar la adecuada gestión de los procesos y servicios a través de métricas de rendimiento y metas para generar valor a la institución y apoyar en el logro de los objetivos y metas institucionales.

La institución debe estar comprometida en la aplicación de buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el cumplimiento de regulaciones internas y externas, así como disposiciones contractuales.

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

La institución debe disponer de informes de resultados sobre las diferentes valoraciones que le permitan identificar desviaciones y áreas de mejora sobre la gestión de TI en la entrega de servicios, la disponibilidad y protección de los recursos tecnológicos. La Unidad de TI debe establecer acciones para el mejoramiento continuo con base en los resultados de las evaluaciones que se deben incorporar a sus planes de trabajo.

La Unidad de TI debe informar formalmente al órgano rector sobre tecnologías de información sobre los resultados de su gestión de acuerdo con los planes establecidos, identificando el nivel de alineación y entrega de valor y beneficios según lo definido para el logro de los objetivos institucionales."

El Lic. Geiner Gamboa Otárola, encargado general del contrato Servicios de Azure Vía Enterprise Agreement y jefe de la Subàrea de Subárea Gestión de Producción de la Dirección de Tecnologías de Información y Comunicaciones, indicó:

"Actualmente, las funciones y responsabilidades asociadas a la administración de la plataforma en la nube han venido en constante crecimiento, debido al aumento progresivo en la complejidad de dicha infraestructura. La operación demanda cada vez más atención y recursos, y el equipo actual no tiene la capacidad suficiente para responder con la agilidad que requiere una institución como la CCSS, especialmente considerando que cada vez más servicios dependen de recursos en la nube.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Un aspecto crítico es que este esfuerzo no cuenta con un equipo humano dedicado exclusivamente a la implementación o migración hacia la nube, lo que agrava la situación. Esta falta de dedicación específica incrementa notablemente la dificultad en términos de administración, control y apropiación técnica, conocimientos que hemos tenido que construir.

Además, lejos de simplificarse, las labores operativas se vuelven complejas aún más por la necesidad de fortalecer la capacitación del equipo. Esta capacitación debe ser verdaderamente efectiva y contar con el tiempo adecuado para lograr un desarrollo real de competencias técnicas. Sin embargo, los funcionarios están comprometidos con la operativa diaria (atendiendo soporte, mantenimiento, reuniones y tareas urgentes), lo cual limita drásticamente su disponibilidad para aprovechar procesos formativos. La única alternativa viable en este contexto sería realizar las capacitaciones fuera del horario laboral, una opción que, si bien podría ser considerada, no resulta ideal ni sostenible.

Reitero, el esfuerzo y/o participación del área como infraestructura, seguridad y redes en el escenario actual exige una mayor dedicación y la incorporación de más personal especializado si se quiere garantizar una operación eficiente, estable y sostenible; pero, la falta de recursos y de un equipo dedicado a imposibilitado el escenario ideal.

(…) Azure cuenta con herramientas integradas que permiten monitorear el uso de los recursos asignados, como espacio, procesamiento y almacenamiento. Sin embargo, para que esta evaluación sea verdaderamente efectiva, es fundamental que los usuarios también participen activamente, brindando retroalimentación al equipo sobre sus necesidades y oportunidades de optimización del recurso tecnológico.

Por mi parte, dispongo de dos personas que asumen múltiples funciones, y solo una fracción de su tiempo puede destinarse a la verificación y seguimiento del uso de los recursos. Esta situación no es la más adecuada, ya que limita la capacidad de realizar un monitoreo continuo y detallado."

La Licda. Vanessa Carvajal Carmona, jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, señalo:

"Es decir, en el ámbito físico ya existía una base consolidada que facilitaba la administración, operación y mantenimiento de la plataforma, incluyendo aspectos como nomenclatura, configuración de equipos, asignación de roles y definición de responsabilidades. Sin embargo, en el entorno de nube, aún no se ha formalizado un cuerpo de mejores prácticas que oriente de manera clara y estructurada la gestión de recursos, configuraciones, seguridad, y otros elementos críticos. Como usted lo menciona, esto representa una oportunidad valiosa para desarrollar lineamientos específicos orientados al entorno de nube, que incluyan la definición de estándares técnicos, políticas de seguridad, así como la asignación clara de roles y responsabilidades entre los distintos equipos involucrados.

(…) A mí sí me preocupa el crecimiento que este proceso está teniendo, especialmente porque no se nos están asignando los recursos humanos necesarios para sostenerlo. Es importante dejar constancia de que, mientras el ecosistema de servicios crece cada día, el número de personas asignadas prácticamente se mantiene igual, lo cual inevitablemente impacta en la capacidad de respuesta. Por ello, hemos insistido repetidamente —y aprovecho para reiterarlo a través de esta entrevista— es necesario considerar el fortalecimiento del equipo humano, para poder seguir soportando adecuadamente el crecimiento tecnológico de la institución.

A nivel de costos, la situación no me preocupa tanto: si bien se reducen gastos en infraestructura física, aumentan en la nube, pero se compensa. Es un equilibrio de costos. Sin embargo, la falta de recurso humano especializado sí es un riesgo importante. Actualmente, estamos creciendo, utilizando prácticamente los mismos recursos de siempre, lo cual no es sostenible en el mediano y largo plazo. (…)

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Yo estimo que la curva de madurez para un dominio adecuado podría ser de unos cinco años. Es preocupante que, aunque desde 2020 se inició el primer contrato de Azure, no se haya avanzado lo suficiente en ese aprendizaje. Durante los primeros 4 años, el proceso estuvo muy centralizado en una sola persona, lo que desaprovechó tiempo valioso para fortalecer capacidades de manera institucional.

Actualmente se ha logrado un avance importante, impulsado principalmente por la gestión de Robert, quien ha promovido el fortalecimiento del equipo mediante el aumento en la cantidad de personas. No obstante, este crecimiento no ha venido acompañado de una definición formal de roles ni de una asignación clara de funciones. Preocupa que estos avances dependan en gran medida de la iniciativa personal de un director, y no de una directriz institucional formal que garantice su continuidad y sostenibilidad en el tiempo. ¿Si mañana Robert ya no estuviera, podríamos retroceder? Por eso yo pienso que la alta dirección de DTIC debe reconocer, respaldar y formalizar la importancia de estos proyectos en la nube, acompañándolos de recursos presupuestarios, humanos, de infraestructura y de un marco normativo robusto."

El Lic. Erick Vindas Umaña, jefe de la Subárea de Seguridad TI de la Direccion de Tecnologías de Información y Comunicaciones, indicó:

"El problema radica en la tendencia de considerar la seguridad como una responsabilidad únicamente nuestra, lo que limita la capacidad de la CCSS para gestionar y supervisar los riesgos de manera adecuada. Como equipo de ciberseguridad, nuestra función principal debería ser la supervisión, validación del cumplimiento y fiscalización, no necesariamente la gestión operativa directa de plataformas o sistemas. Sin embargo, debido a la falta de recursos y personal, hemos tenido que asumir tareas que no corresponden a nuestro rol original, como desarrollar y definir redes o infraestructuras que pertenecen más a otras áreas especializadas.

Este tipo de implicación es comprensible porque somos un equipo, pero no debe desvirtuar la responsabilidad central de ciberseguridad, que debe centrarse en la validación y el cumplimiento, no en la ejecución operativa de las plataformas. Si bien la ciberseguridad debe adaptarse a los cambios, debemos ser conscientes de que existen límites claros en cuanto a nuestra área de competencia.

(…) Actualmente, se están aplicando herramientas de correlación de eventos, control de acceso, control de casos de uso (SIEM) y, de manera preventiva, el análisis de vulnerabilidades, así como la visualización del comportamiento a través del EDR de los servidores desplegados en la nube. Básicamente, las medidas de protección definidas en el WAF de Cloud Guard, correspondientes a la seguridad perimetral en entornos de nube, están siendo implementadas de manera adecuada. Sin embargo, el monitoreo periódico sigue siendo un desafío, debido a que aún no existe una madurez institucional suficiente que permita aplicar de forma continua las mejoras necesarias.

Además, se evidencia que las propias cargas de trabajo actuales limitan la capacidad de refinamiento y optimización de estos controles de seguridad.

(…) Agregaría que, en algunas ocasiones, se han implementado soluciones a través de la plataforma de nube, acompañadas de capacitaciones sobre el uso de la herramienta. Si bien hemos participado en estas capacitaciones, a menudo no se especifica con claridad quién es responsable de realizar cada tarea dentro del proceso. Esto genera incertidumbre sobre la administración de las soluciones, que sólo se clarifica una vez que la herramienta ya está en funcionamiento. Es en ese momento cuando empiezan a evidenciarse deficiencias, ya sea porque algunas áreas no se involucran adecuadamente o porque otras asumen tareas adicionales para dar soporte. En este sentido, considero que una oportunidad de mejora clara es fortalecer la planificación previa a la implementación de productos, asegurando que se definan de manera explícita y consensuada de roles y tareas de cada área especialista dentro de la DTIC."

La persistencia de limitaciones en la capacidad operativa, dedicación de personal, disponibilidad presupuestaria y gestión del conocimiento técnico representa una amenaza directa para la sostenibilidad y evolución de los

servicios tecnológicos institucionales. En ese orden de ideas, si no se abordan estas brechas de manera integral, la CCSS enfrentará una creciente dificultad para responder con agilidad a las demandas estratégicas, limitará su capacidad de innovación y aumentará su exposición a riesgos operacionales y de continuidad.

Además, la falta de procesos sistemáticos de monitoreo, optimización y adopción de buenas prácticas dificultará la eficiencia en el uso de recursos, reduciendo el retorno de inversión y el impacto esperado de la transformación digital, aspectos que comprometen no solo la eficiencia técnica, sino también la competitividad y resiliencia institucional a largo plazo.

6. SOBRE LA ACTUALIZACIÓN DEL CONOCIMIENTO Y CAPACITACIÓN

No se obtuvo evidencia de la existencia de programas de capacitación masivos o estructurados orientados a generar conocimiento institucional sobre los servicios de computación en la nube. Según lo detallado en el oficio GG-DTIC-1939-2025 del 27 de marzo de 2025 suscrito por el Máster Robert Picado Mora, subgerente de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), en el marco de la estrategia de implementación de la nube Azure, se promovieron seis sesiones con un arquitecto de nube de Microsoft, en las cuales se abordarían temas con objetivos específicos. Estas sesiones fueron comunicadas a 15 funcionarios que integran el equipo de arquitectura tecnológica, así como a los jefes de área y Subarea de la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

En otras palabras, las acciones realizadas hasta el momento por dicha Dirección han estado enfocadas principalmente en sus propias unidades internas, mediante el aprovechamiento de los contratos vigentes con el fabricante Microsoft y su plataforma Azure.

A ese respecto, se consultó a diversas unidades programáticas externas a la DTIC que ya han completado o se encuentran en proceso de migración hacia la nube, como resultado, un 50% de estas unidades manifestó no haber recibido capacitación formal en el uso y administración de servicios en la nube, mientras que un 33% indicó que dicha capacitación no les era aplicable. Además, se destacaron comentarios como el siguiente: *"Este es un tema nuevo para las unidades de la Caja. Muchas de ellas no tienen conciencia de lo que implica trabajar y almacenar productos en la nube, por lo que, en ocasiones, no reciben el apoyo administrativo necesario, ya que se percibe como un asunto exclusivo de las TIC. Sin embargo, esto involucra aspectos de costos y datos que pertenecen a los usuarios"*; otro comentario relevante *"Considero que todos los involucrados deben estar al tanto de temas como la seguridad en la nube y el almacenamiento de datos en este entorno. Es crucial que se entienda que no todo puede ser subido a la nube y que se debe evaluar cuidadosamente. Además, contar con productos en la nube conlleva un costo operativo que el usuario final desconoce y que debería asumir"*; observaciones que refuerzan la necesidad de actualización y capacitación continua en los temas relacionados con la gestión de la nube, tanto en términos operativos como estratégicos.

Por otro lado, en las unidades de la DTIC que sí han accedido a procesos de actualización del conocimiento, no se ha logrado un aprovechamiento óptimo, debido a que las labores operativas cotidianas limitan significativamente la disponibilidad del personal para participar activamente en dichas capacitaciones.

Por lo tanto, la oportunidad de mejora radica en asegurar que las acciones de capacitación promuevan una actualización de conocimientos más amplia y efectiva entre el personal que, por sus funciones, requerirá competencias específicas para respaldar los procesos de adopción, implementación y gestión de soluciones en la nube.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT los apartados correspondientes al X. "Desarrollo, Implementación y Mantenimiento de Sistema de Información y "Administración Infraestructura tecnológica", señala:

> *"La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o*

involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales"

Esas mismas Normas en su apartado XI. Seguridad y Ciberseguridad, señala que:

"La Institución debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios, contemplando contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."

El Lic. Geiner Gamboa Otárola, encargado general del contrato Servicios de Azure Vía Enterprise Agreement y jefe de la Subàrea de Subárea Gestión de Producción de la Dirección de Tecnologías de Información y Comunicaciones, indicó:

"(…) lejos de simplificarse, las labores operativas se vuelven complejas aún más por la necesidad de fortalecer la capacitación del equipo. Esta capacitación debe ser verdaderamente efectiva y contar con el tiempo adecuado para lograr un desarrollo real de competencias técnicas. Sin embargo, los funcionarios están comprometidos con la operativa diaria (atendiendo soporte, mantenimiento, reuniones y tareas urgentes), lo cual limita drásticamente su disponibilidad para aprovechar procesos formativos. La única alternativa viable en este contexto sería realizar las capacitaciones fuera del horario laboral, una opción que, si bien podría ser considerada, no resulta ideal ni sostenible."

La Licda. Vanessa Carvajal Carmona, jefe del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, señalo:

"Es decir, sí tenemos personal que puede realizar las funciones, pero en muchos casos hablamos de una sola persona por área crítica. Por ejemplo: Para implementar un servidor, hay solo una persona disponible; para configuraciones de seguridad, solo una persona; para temas de redes, igualmente una persona.

Esta limitación genera que, aunque se tenga la capacidad técnica, el volumen de trabajo y la poca disponibilidad de manos hace que los tiempos de respuesta no siempre sean los ideales. Un requerimiento que en condiciones normales podría resolverse en uno o dos días, puede tardar hasta una semana o más, debido a la carga operativa diaria que también deben atender.

Muchos estamos aprendiendo sobre la marcha, y si bien hay compromiso, la falta de capacitación especializada limita la respuesta técnica. Es urgente que cada equipo reciba capacitación puntual en las herramientas y áreas específicas que les competen.

Podríamos decir que en la DTIC sí contamos con personal capacitado, pero no en la cantidad suficiente para asumir de manera óptima el crecimiento de servicios en la nube."

El Lic. Erick Vindas Umaña, jefe de la Subárea de Seguridad TI de la Direccion de Tecnologías de Información y Comunicaciones, indicó:

"Además, si consideramos casos algunos casos de personal, vemos que se mantienen a base de sustituciones, por lo cual en cualquier momento se deja de contar con el recurso. Esto evidencia otro problema: no todos los recursos disponibles cuentan con el conocimiento, la creatividad o la experiencia necesarios para enfrentar ciertas tareas complejas. Esto, a su vez, afecta la capacidad o la posibilidad de mantener el ritmo ante la creciente cantidad de temas y desafíos que se van generando, lo que termina por incidir negativamente en la calidad del trabajo.

(…) Agregaría que, en algunas ocasiones, se han implementado soluciones a través de la plataforma de nube, acompañadas de capacitaciones sobre el uso de la herramienta. Si bien hemos participado en estas capacitaciones, a menudo no se especifica con claridad quién es responsable de realizar cada tarea dentro

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

del proceso. Esto genera incertidumbre sobre la administración de las soluciones, que sólo se clarifica una vez que la herramienta ya está en funcionamiento. Es en ese momento cuando empiezan a evidenciarse deficiencias, ya sea porque algunas áreas no se involucran adecuadamente o porque otras asumen tareas adicionales para dar soporte. En este sentido, considero que una oportunidad de mejora clara es fortalecer la planificación previa a la implementación de productos, asegurando que se definan de manera explícita y consensuada de roles y tareas de cada área especialista dentro de la DTIC."

En ese sentido, la situación actual impide que los funcionarios puedan destinar tiempo de manera enfocada a su desarrollo profesional, limitando la profundización en aspectos técnicos esenciales, dificultando la especialización necesaria para fortalecer el desempeño del equipo.

Por ende, la situación observada en cuanto al desarrollo de procesos de formación, capacitación y actualización técnica en esta materia podrían, a mediano plazo, derivar en esfuerzos fragmentados y desarticulados en la adopción de la tecnología; propiciando la concentración del conocimiento en áreas o funcionarios puntuales, sin contar con mecanismos efectivos para su transferencia, escalabilidad o sostenibilidad institucional, lo cual restringe la capacidad de la organización para gestionar de manera integral esta solución tecnológica de nube con el fin de aprovechar plenamente sus beneficios.

7. SOBRE LA NECESIDAD DE REVISIÓN Y ACTUALIZACIÓN DE LA MATRIZ DE RIESGOS ASOCIADOS CON COMPUTACIÓN EN LA NUBE

Se determinó que el proceso de identificación de riesgos tecnológicos relacionados con la gestión del Centro de Datos en la Nube, contenido en el Plan de Continuidad elaborado exclusivamente por la Subárea de Gestión de Producción de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), contempla únicamente cuatro riesgos específicos. Esta limitación evidencia que dicho análisis no ha sido abordado de forma integral ni con la participación de otras unidades técnicas, lo cual reduce su alcance y efectividad frente a la complejidad del entorno tecnológico en la nube.

Cuadro No. 6
Identificación de riesgos, Subárea Gestión de Producción
Gestión de Data Center de Nube, 2025

Amenazas	Vulnerabilidad	Riesgo	Impacto	Nivel de Riesgo	Riesgo residual
Falla de proveedor externo	Interrupciones en la comunicación, perdida de acceso a la información, impacto en la proactividad y aumento de riesgo.	Interrupción de comunicación de express route.	Interrupción total de las comunicaciones de nube.	ALTO	Falla o interrupción de servicio
Alta demanda de actividades en la Subárea	Alta carga de trabajo debido a la mayor demanda de actividades y exigencia operativa del personal de la subárea en la gestión de Datacenter.	Que no haya personal disponible para realizar las labores técnicas y de gestión.	Retrasos en la atención de solicitudes a la Subárea	ALTO	Atención no oportuna.
Falta de personal.	Falta de personal por la alta carga de trabajo debido a la mayor demanda de actividades y exigencia operativa del personal de la subárea	No se podrían ejecutar ningún tipo de labor en el II y III turno	Los problemas suscitados en horario fuera de oficina deberán esperar al siguiente día hábil para su atención y resolución.	MEDIO	Dependencia de terceros

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Amenazas	Vulnerabilidad	Riesgo	Impacto	Nivel de Riesgo	Riesgo residual
Falla de software (lógico)	Afectación en la integridad de los datos y accesos, interrupción de servicios, materialización de vulnerabilidades, impacto en la plataforma y otros daños colaterales generados por un ciberataque.	Afectación parcial o total de la plataforma tecnológica que contempla los sistemas de almacenamiento, respaldo, de conectividad, servidores virtuales.	Interrupción parcial o total de la plataforma tecnológica que contempla los sistemas de almacenamiento, respaldo, de conectividad, servidores virtuales y físicos.	ALTO	Dependencia de terceros para la atención de la interrupción de servicio

Fuente: Adjunto al oficio GG-DTIC-1939-2025 del 27 de marzo de 2025, Plan de Continuidad.

Como se puede observar, presentan un nivel básico de desarrollo, ya que no abordan de manera integral una serie de riesgos críticos asociados con la operación y administración de entornos en la nube. A manera de ejemplo, se detalla a continuación factores no considerados en listado anterior:

- Dependencia de proveedores de servicios en la nube específicos y/o exposición a costos adicionales asociados con la recuperación, migración o reinstalación de datos en otras plataformas o infraestructuras locales.

- Riesgos regulatorios y de cumplimiento, especialmente relevantes por el manejo de información sensible en el contexto institucional.

- Error humano en la configuración de servicios, que puede derivar en la caída de sistemas o exposición de datos sensibles.

- Fallos en actualizaciones automáticas, los cuales podrían generar interrupciones de servicio o incompatibilidades con otros componentes de la infraestructura.

- Fugas de información por accesos indebidos, derivadas de configuraciones incorrectas de permisos o de una gestión deficiente de identidades.

- Uso no autorizado de recursos, que podría generar vulnerabilidades de seguridad, incumplimientos normativos y costos operativos no previstos.

- Riesgo financiero por consumo descontrolado, asociado a una gestión ineficiente o errónea del dimensionamiento y automatización de recursos en la nube.

En ese sentido, la omisión de estos elementos compromete la efectividad del análisis de riesgos y limita la capacidad institucional para anticiparse, mitigar y responder adecuadamente ante eventos que pueden impactar significativamente la continuidad del servicio, la seguridad de la información y el cumplimiento normativo.

La Ley General de Control Interno No. 8292, en el numeral 14 establece que para la “Valoración de Riesgo”, será deber de los titulares subordinados lo siguiente:

> *“a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.*
> *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.*
> *c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.*

d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar."

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT, en el apartado XII. Administración Infraestructura Tecnológica, cita que:

> *"La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados. Adicionalmente, debe asegurar que las unidades institucionales disponen y aplican practicas e instrumentos que le permitan evaluar la adecuada gestión de los procesos y servicios a través de métricas de rendimiento y metas para generar valor a la institución y apoyar en el logro de los objetivos y metas institucionales."*

Dentro de las causas de la situación descrita, es criterio de esta Auditoría que responde a la limitada madurez institucional en la gestión estratégica de tecnologías emergentes, particularmente en lo relativo a infraestructura cloud. Esta condición se explica, entre otros factores, por capacidades técnicas insuficientes para identificar y administrar riesgos específicos de este tipo de plataformas, la ausencia de metodologías actualizadas orientadas a su adecuada gobernanza, la falta de integración efectiva entre áreas clave, así como por un enfoque predominantemente operativo y reactivo, que prioriza la ejecución técnica sobre la gestión preventiva.

Todo lo anterior ha derivado en un abordaje carente de profundidad e integralidad en el análisis de riesgos, lo cual compromete la capacidad institucional para anticipar, mitigar y responder de manera eficaz ante eventos que puedan afectar la continuidad operativa, la seguridad de la información y el cumplimiento de marcos normativos

Como consecuencia de la falta de una gestión de riesgos adecuada, la CCSS se ve expuesta a amenazas críticas que ponen en riesgo la integridad de la información, la disponibilidad de los servicios y la estabilidad tecnológica, lo que se puede traducir en un debilitamiento de la capacidad institucional para anticipar incidentes, aumentando la probabilidad de eventos como ataques cibernéticos, interrupciones de servicios esenciales y la posible pérdida de datos clave, lo que pone en peligro la operatividad y la seguridad de los sistemas.

CONCLUSIONES

La infraestructura tecnológica en nube 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.

A través del presente estudio, esta Auditoría identificó diversas oportunidades de mejora relacionadas con la gestión de servicios, configuración, normativa y seguridad de esa plataforma en nube, cuyo abordaje resulta esencial para asegurar la continuidad operativa, la eficiencia institucional y la alineación estratégica de los servicios tecnológicos.

A ese respecto, la Institución dispone de una estrategia integral para la gestión de su plataforma tecnológica en la nube. No obstante, según las observaciones emitidas, se evidenció la necesidad de fortalecer dicha estrategia y/o los planes de acción detallados que le permitan maximizar el aprovechamiento de los recursos institucionales, bajo principios de sostenibilidad y disponibilidad, orientados al cumplimiento de la ruta tecnológica definida.

Sin embargo, se constató que la cartera de proyectos contemplada en la "Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube" no ha sido incorporada en los instrumentos de planificación institucional vigentes en materia de tecnologías de información; situación que podría estar afectando negativamente el seguimiento, control y administración de los recursos asignados a dichos proyectos.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Pese a la envergadura, el impacto esperado de estas iniciativas y los recursos comprometidos entre los años 2024 y 2028, se observa una falta de alineación con la Agenda Digital Institucional (AGEDI) y con el Banco de Iniciativas Estratégicas. Esta desconexión adquiere mayor relevancia al considerar las inversiones realizadas en el periodo 2021-2023, que superan los $2.751.077,36 (dos millones setecientos cincuenta y un mil setenta y siete dólares con 36/100), así como la estimación proyectada de $15.854.378,62 (quince millones ochocientos cincuenta y cuatro mil trescientos setenta y ocho dólares con 62/100), en caso de ejecutarse la hoja de ruta en su totalidad. A ello se suma la dependencia crítica que muchas unidades de negocio tanto sustantivas como de apoyo tienen de dicha infraestructura tecnológica.

Por otro lado, la ausencia de una estructura normativa integral para la adopción de servicios en la nube representa una oportunidad significativa de mejora. La definición de pautas y regulaciones claras para la adquisición, uso y administración del entorno en la nube contribuiría a mitigar riesgos, optimizar el uso de los recursos y promover una implementación ordenada y sostenible de la tecnología.

El análisis también evidenció debilidades en las capacidades institucionales para administrar eficientemente los servicios en la nube, destacando: limitaciones en la capacidad técnica del recurso humano, escasa articulación entre áreas, dependencia de personal clave, restricciones contractuales, ausencia de monitoreo proactivo, velocidad para adoptar buenas prácticas, así como deficiencias en los procesos de seguridad y estandarización. Tales hallazgos comprometen la sostenibilidad, eficiencia y evolución de la plataforma, por lo que resulta imperativo fortalecer los mecanismos de gobernanza, planificación, gestión de riesgos y capacidades técnicas institucionales.

Asimismo, se identificó la necesidad de establecer una metodología que permita identificar, clasificar y priorizar adecuadamente las necesidades tecnológicas, ante el crecimiento proyectado de las unidades usuarias]; proceso deberá ser liderado por la DTIC en colaboración y/o participación de los Centros de Gestión Informática, dentro de sus posibilidades operativas.

Finalmente, este Órgano Fiscalizador considera que la gestión de riesgos constituye un componente esencial para el cumplimiento de los objetivos institucionales, ya que permite identificar amenazas potenciales y adoptar medidas para prevenirlas o mitigarlas oportunamente. En ese sentido, se determinó la necesidad de fortalecer la cultura institucional en torno a la gestión de riesgos y robustecer las herramientas de control actualmente disponibles. Particular atención debe prestarse a los riesgos asociados a la plataforma tecnológica en la nube, los cuales requieren un tratamiento sistemático que abarque los niveles estratégico, táctico y operativo, mediante procesos eficaces de identificación, análisis, valoración, tratamiento, comunicación y seguimiento.

En virtud de lo anterior y en conformidad con el marco regulatorio aplicable, esta Auditoría propone una serie de recomendaciones con el fin de que sean consideradas por la administración para coadyuvar en la mitigación de los riesgos identificados en el presente estudio, lo anterior en aras de fortalecer la gestión de Servicios, Configuración, Normativa y Seguridad en la Nube.

RECOMENDACIONES

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

1. De conformidad con lo señalado en el hallazgo 1, valorar la inclusión de la cartera de proyectos contemplada en la “Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube” dentro de los mecanismos de control institucional aplicables a la planificación de proyectos y/o iniciativas con componentes tecnológicos, con el propósito de facilitar su adecuado seguimiento y monitoreo, según el nivel de complejidad e impacto que presenten.

   Es importante señalar que el análisis y las medidas que se adopten deberán implementarse en estricto cumplimiento de la normativa vigente aplicable en la materia. Una vez finalizada la valoración, se deberá

informar al Consejo Tecnológico Institucional sobre los ajustes realizados, asegurando que se establezca un mecanismo de control adecuado para el seguimiento y monitoreo del conjunto de proyectos involucrados, máxime considerando el impacto, la cobertura y la cuantía de los proyectos.

Para acreditar el cumplimiento de lo recomendado remitir a la Auditoría en el plazo de **5 meses** posterior a la recepción de este informe, la documentación donde conste el análisis realizado, las acciones adoptadas para la inclusión del conjunto de proyectos en el mecanismo de control que corresponda y la comunicación efectuada al Consejo Tecnológico Institucional.

2. Respecto a la "Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube", fortalecer su contenido o, en su defecto, complementarlo con un plan de acción suficientemente detallado que contribuya a la materialización efectiva de sus objetivos estratégicos, incorporando las observaciones señaladas en el Hallazgo 2 del presente informe, así como lo solicitado por el Consejo Tecnológico Institucional. Lo anterior considerando, al menos, los siguientes aspectos:

   - Realizar un diagnóstico integral de las condiciones actuales en relación con los servicios en la nube, considerando las capacidades técnicas, organizativas, normativas y del talento humano. Este diagnóstico tiene como finalidad identificar brechas críticas que puedan comprometer la implementación. Con base en sus resultados, se deberá valorar la necesidad de establecer actividades específicas para subsanar dichas brechas antes de ejecutar los proyectos definidos en la "Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube".

   - Asegurar la participación temprana y activa de los actores del negocio, como responsables funcionales de sistemas críticos institucionales, promoviendo una visión compartida, una adecuada gobernanza y una alineación efectiva con los objetivos estratégicos.

   - Desarrollar un esquema claro de gestión de riesgos, que permita anticipar amenazas clave y establecer mecanismos de mitigación alineados con la complejidad de los proyectos contemplados.

   - Detallar las actividades a desarrollar, sus responsables, plazos y métricas de éxito específicas, a fin de facilitar su monitoreo, priorización y evaluación.

   - Generar insumos con la valoración integral de los entornos multi-nube, considerando aspectos clave como la interoperabilidad, portabilidad, contratación, gobernanza y sostenibilidad. Asimismo, definir una estrategia para la selección tecnológica que oriente, las decisiones de la CCSS entre distintas soluciones en la nube, respaldando una toma de decisiones estratégica sobre tecnologías y proveedores, y reduciendo el riesgo de dependencia hacia casas comerciales específicas.

   Una vez concluida la labor realizada, se deberá informar al Consejo Tecnológico Institucional al respecto, considerando que este ya tuvo conocimiento previo de la estrategia. De esta forma, el Consejo podrá revisar el documento, aportar mejoras y realizar los ajustes correspondientes, con el fin de autorizar su oficialización y promover, mediante una directriz institucional, la importancia del proyecto y la disposición existente para atender las necesidades tanto a nivel central como regional y local.

   Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización, en un plazo de **6 meses** a partir de la recepción del presente informe, la documentación que respalde el análisis de las observaciones supracitadas, así como las acciones ejecutadas para el fortalecimiento de la "Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube" o, en su defecto, del plan de acción que se haya definido al respecto; en cualquiera de los casos, la documentación deberá estar debidamente socializada.

3. En atención a los hallazgos 3 y 5 del presente informe, y en alineamiento con las gestiones para la actualización de procesos impulsada por la Dirección de Tecnologías de Información y Comunicaciones

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

mediante el proyecto "*Modelo Meta de Gobernanza y Gestión de las TIC"*, revisar, modificar y/o actualizar el marco normativo que refiere al proceso de computación en la nube, en aras de que éstos respondan a la realidad actual de la institución en materia de garantizar la prestación de servicios tecnológicos.

Teniendo en cuenta que la Recomendación 2 del Informe ATIC-0080-2024, dirigido al Consejo Tecnológico y relativo a la "Auditoría de carácter especial sobre la gestión de las tecnologías emergentes en la CCSS", contempla la formulación de un marco normativo institucional para la gestión de dichas tecnologías, y considerando que su desarrollo podría requerir un proceso gradual, se solicita valorar la definición anticipada de elementos clave que orienten la gestión operativa de los servicios en la nube.

En este sentido, resulta necesario disponer, a la mayor brevedad, de documentación consensuada que respalde la asignación clara de tareas, roles y responsabilidades de los actores involucrados; el establecimiento de lineamientos técnicos básicos para la configuración, operación y mantenimiento de las plataformas en la nube; así como la implementación de mecanismos eficaces para su supervisión y monitoreo. Todo lo anterior, sin perjuicio de que, en una etapa posterior, estos aspectos sean integrados dentro de un marco normativo consolidado que aborde de forma integral la gestión institucional de la computación en la nube.

Para acreditar el cumplimiento de la presente oportunidad de mejora, debe remitirse a esta Auditoría en un plazo de **6 meses** a partir de la fecha de recepción del estudio, la documentación que respalde la valoración realizada sobre el marco regulatorio vigente, así como los planes definidos para la oficialización anticipada de elementos clave que orienten la gestión operativa de los servicios en la nube.

4. A partir de la situación institucional descrita en el Hallazgo 4, y en alineamiento con la vinculación existente entre la compra No. 2024LY-000005-0001101161 "Servicios de Azure Vía Enterprise Agreement" y los objetivos establecidos en la "Hoja de Ruta: Estrategia de Habilitación y Migración de Servicios en la Nube", fortalecer la planificación y estimación institucional de necesidades vinculadas al consumo de servicios en la nube.

   Para ello, deberá diseñarse e implementarse una metodología formal, integral y participativa para la proyección de requerimientos tecnológicos asociados a contrataciones de servicios en la nube; considerando, como mínimo:

   a) Análisis detallado y articulado entre la infraestructura tecnológica actual y las proyecciones de migración de esos servicios a la nube, considerando escenarios de corto, mediano y largo plazo.
   b) Priorización de soluciones institucionales según criterios técnicos, operativos y estratégicos.
   c) Estimación de los recursos tecnológicos necesarios para cada solución o iniciativa, incluyendo cantidad, tipo de servicio en la nube requerido y capacidad proyectada, con base en criterios técnicos y operativos que respalden su justificación.
   d) Participación de los Centros de Gestión Informática (CGI) y unidades de negocio relevantes, de forma que se garantice la alineación entre necesidades locales y decisiones de inversión tecnológica.

   Para acreditar el cumplimiento de esta recomendación, debe enviarse a este Ente Fiscalizador en un plazo de **9 meses** a partir de la fecha de recepción del presente informe, la valoración de la atención de los puntos a, b, c y d antes señalados, así como los insumos y gestiones realizadas o previstas para fortalecer la planificación y estimación institucional de las necesidades asociadas al consumo de servicios en la nube.

5. En atención a las debilidades identificadas en la administración de la infraestructura en la nube, descritas en el hallazgo 5 y cuyo impacto trasciende a nivel institucional, establecer desde esa Dirección, y en coordinación con las jefaturas de las áreas y subáreas competentes, un plan integral de mejora que fortalezca la gestión operativa y administrativa de los servicios en la nube, abarcando de manera estructurada las siguientes áreas clave:

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

a) Evaluar la viabilidad y necesidad de actualizar los programas institucionales, como el de Gobernanza y Gestión de las TIC, Hoja de Ruta del Plan de Ciberseguridad, entre otras iniciativas que estimen pertinentes, con base en los avances actuales y futuros en el uso de tecnologías de computación en la nube.
b) Optimizar las condiciones del equipo técnico asignado a soportar la nube, asegurando la transformación de habilidades e impulsando una mayor cohesión y capacidad de respuesta mediante la asignación de personal. De manera que se fomente un enfoque multidisciplinario y garantizar la transferencia de conocimiento técnico entre los miembros del equipo, para reducir la dependencia de determinados recursos.
c) Verificar que el administrador del contrato de los servicios de Azure cuente con las capacidades técnicas, operativas y de gestión necesarias para desempeñar de manera efectiva su rol, el cual comprende, entre otras funciones, el seguimiento contractual; la gestión del consumo y control presupuestario; la coordinación técnica y operativa con equipos internos y el proveedor; la elaboración y resguardo de documentación de soporte; la atención de incidentes y no conformidades; la validación de entregables y emisión de conformidades de servicio; así como su participación activa en comités o mesas de trabajo y en los procesos de planificación para futuras renovaciones o contrataciones relacionadas.
d) Implementar un sistema de monitoreo continuo, proactivo y programado que permita evaluar de forma oportuna el desempeño operativo de la plataforma en la nube, gestionar alertas de seguridad en tiempo real, y generar informes periódicos sobre vulnerabilidades, entre otros insumos que permitan aumentar la capacidad de respuesta, prevenir incidentes y garantizar la disponibilidad, integridad y confiabilidad de los servicios tecnológicos.
e) Impulsar con mayor celeridad la adopción de buenas prácticas en la gestión de los entornos en la nube, orientadas a obtener un mayor nivel de madurez en el uso y aprovechamiento de la plataforma, fomentando la estandarización de procesos, el aprovechamiento integral de funcionalidades, la eficiencia operativa, la optimización de recursos y la mejora continua.

Para acreditar el cumplimiento de esta recomendación, debe enviarse a este Ente Fiscalizador en un plazo de **9 meses** a partir de la fecha de recepción del presente informe, el plan de mejora que respalde la atención de los puntos a, b, c, d y e, así como evidencia de su socialización con las partes involucradas.

6. En concordancia con las necesidades de capacitación, formación y actualización del conocimiento señaladas en el hallazgo 6, coordinar con las instancias pertinentes la elaboración e implementación de un plan de acción que asegure que todos los actores involucrados (a nivel central, regional y local) en la gestión de servicios en la nube cuenten con las competencias requeridas, según su nivel de responsabilidad y participación.

   En ese sentido, el plan deberá incluir acciones orientadas a fortalecer el conocimiento general (actual y necesidades futuras) sobre esta tecnología en los personal técnico y especializado; personal de desarrollo de software y gestión de aplicaciones; personal administrativo y de gestión; usuarios funcionales o usuarios finales; promoviendo así su apropiación y aprovechamiento.

   Estos recursos deberán canalizarse mediante procesos formativos que incluyan certificaciones formales o, en su defecto, mecanismos como sesiones informativas, talleres, entrenamientos, videoconferencias y plataformas de aprendizaje virtual, entre otros medios. Asimismo, será fundamental establecer controles que permitan evidenciar qué funcionarios han participado efectivamente en dichas actividades de capacitación, así como definir con claridad el compromiso de estos para asumir un rol activo y responsable en el soporte y la gestión operativa de la plataforma en la nube.

   Para acreditar el cumplimiento de esta oportunidad de mejora, deberá remitirse a esta Auditoría, en un plazo de **8 meses** a partir de la fecha de recepción del presente estudio, el plan de acción debidamente aprobado por el Despacho de la Dirección de Tecnologías de Información y Comunicaciones, junto con la instrucción formal para su implementación.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

7. De conformidad con lo señalado en el hallazgo 7 de este informe, revisar y, en caso de corresponder, actualizar los documentos elaborados por esa Dirección, así como por las jefaturas de las áreas y subáreas competentes, que contengan o deban contener matrices de riesgos relacionadas con la computación en la nube.

   Dicha revisión debe garantizar que dichos instrumentos incorporen de manera pertinente los aspectos vinculados a este entorno tecnológico, conforme a los riesgos actuales y las mejores prácticas en la materia. En este contexto, se debe refinar la identificación de riesgos, incorporando un enfoque integral que contemple la totalidad de riesgos aplicables, estableciendo los controles mínimos necesarios para su mitigación y definiendo una metodología clara para el monitoreo periódico de su cumplimiento y efectividad.

   Para acreditar el cumplimiento de esta recomendación, debe enviarse a este Ente Fiscalizador en un plazo de **4 meses** a partir de la fecha de recepción del presente informe, la documentación que respalde la valoración efectuada, así como la versión actualizada de la(s) matriz(es) de riesgos asociadas a el tema de computación en la nube.

En relación con las recomendaciones expuestas en el presente informe, en el plazo de 10 días hábiles[16] se deberá remitir a esta Auditoría el "cronograma"[17] con las actividades o tareas, encargados designados y tiempo de ejecución previstos en función del plazo total acordado para el cumplimiento de cada una. Asimismo, informar periódicamente sobre los avances del cronograma y aportar las evidencias respectivas, a fin de que se pueda verificar el cumplimiento oportuno.

Se recuerda que, si por motivos debidamente justificados, durante la ejecución del cronograma la administración requiere ampliar el plazo de alguna recomendación, el jerarca o titular subordinado responsable de su cumplimiento, deberá solicitar formalmente la respectiva prórroga, en tiempo y forma, conforme lo establecido en el artículo 93 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, aportando además, el cronograma actualizado, conforme con el nuevo plazo que se esté solicitando y las actividades que presenten el respectivo retraso justificado.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 62 del Reglamento de Organización y Funcionamiento de la Auditoría Interna de la CCSS, los resultados del presente estudio fueron comentados el 6 de mayo del 2025, de conformidad con oficio de convocatoria AI-0693-2025, con los siguientes funcionarios: Master Robert Picado Mora, Subgerente Dirección de Tecnologías de Información y Comunicaciones; Lic. Geiner Gamboa Otárola, Jefe Subárea Gestión de Producción y Administrador del Contrato No. 2024LY-000005-0001101161 "Servicios de Azure Vía Enterprise Agreement"; Licda. Vanessa Carvajal Carmona, Jefe Área de Soporte Técnico, Dirección de Tecnologías de Información y Comunicaciones. y por parte de la Auditoría Interna: Ing. Leonardo Diaz Porras, jefe a.i del Área Auditoría Tecnologías de Información y Comunicaciones, Ing. Oscar Mena Granados, asistente de auditoría y la Sra. Heidi Peña Alán, asistente de la subárea de seguimientos.

A continuación, se detallan los comentarios emitidos por la Administración Activa y las respectivas respuestas proporcionadas por la Auditoría Interna:

Hallazgo 1: Sobre la cartera de proyectos indicados en la "Hoja de ruta estrategia de habilitación y migración de servicios en nube".

Robert Picado Mora: Solo quería aclarar que esto no se ha incluido aún a la Agenda Digital, porque nuestro objetivo inicial era presentarlo ante el Consejo Tecnológico. Ese tema ya fue llevado allí, no sé si ustedes

[16] Plazo máximo establecido en la Ley General de Control Interno (Art. 17 inciso d / Art. 36 inciso a), para iniciar la implantación de las recomendaciones de los informes de auditoría.
[17] Requerido en el Art. 68 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, el cual hemos denominado en el SIGA: "Cronograma de acciones para el cumplimiento de recomendaciones".

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

están al tanto. A partir de esa presentación, la idea sería emitir las instrucciones correspondientes para su implementación.

Hallazgo 2: Sobre la iniciativa de habilitación y migración de servicios en la nube.
Robert Picado Mora: Ahí sí discrepo, porque en realidad el tema sí se presentó ante el Consejo de los CGIs. De hecho, se expuso en dos etapas: primero ahí y luego se llevó al Consejo, incluso presentando un caso de éxito, que fue el caso de Pensiones.

Oscar Mena Granados: Precisamente, en la estrategia no queda evidencia de ese tipo de socialización ni de la integración de las partes interesadas en el proyecto. Solo se hace referencia al equipo técnico responsable de su ejecución.

Con respecto a los hallazgos 3, 4, 5, 6 y 7, no se emitieron comentarios por parte de la Administración.

Recomendación 1:

Robert Picado Mora: Podríamos alinear el plazo de la recomendación para que coincida con la presentación de avances que tenemos ante el Consejo Tecnológico. Propondría dejarlo en 5 meses.

Vanessa Carvajal Carmona: Yo le había comentado a Óscar, durante nuestra conversación sobre la cartera de proyectos, que esto debe entenderse como una estrategia de servicios a Nube que involucra varios proyectos, algunos de los cuales corresponden a temas muy operativos o adquisiciones puntuales. En ese sentido, aunque AGEDI está vinculado a una cartera de proyectos dentro del Fondo de Inversión, no todos los componentes de esta estrategia están incluidos, ya que no todos califican formalmente como proyectos, sino que algunos se gestionan como compras u operaciones específicas. Esa es precisamente mi inquietud respecto a la recomendación que se está planteando.

Óscar Mena: Aclara que la recomendación queda abierta para que se realice una valoración sobre la incorporación de los distintos proyectos dentro del esquema de control que corresponda, garantizando así un seguimiento razonable de todas las iniciativas incluidas en esta estrategia.

Robert Picado Mora: Coincide en que es necesario revisar el marco normativo. Si por alguna razón ciertos elementos no pueden incorporarse formalmente como proyectos, el control y seguimiento deben mantenerse igualmente. En ese sentido, la recomendación resulta útil para asegurar medidas de seguimiento, incluso cuando se trata de componentes gestionados dentro del presupuesto operativo. Lo importante es asegurar una visión integral de toda la estrategia, más allá de la clasificación formal de cada elemento. Esto puede gestionarse de forma adecuada.

Leonardo Díaz Porras: Acepta la observación y establece el plazo de atención en 5 meses.

Recomendación 2:

Robert Picado Mora: Podríamos cambiar la redacción en relación con el diagnóstico, en la parte que dice “Con base en sus resultados, se deberá valorar la necesidad de establecer actividades específicas para subsanar dichas brechas antes de ejecutar los proyectos (…)” dado que la ejecución de los proyectos ya ha iniciado.

Oscar Mena Granados: Quería así “Con base en sus resultados, se deberá valorar la necesidad de establecer actividades específicas para subsanar las brechas identificadas, a fin de evitar que estas afecten la ejecución de los proyectos. (…)”

Robert Picado Mora y Geiner Gamboa Otárola: ¿Podríamos tener como plazo de la recomendación, 6 meses?

Leonardo Díaz Porras: Acepta la observación y establece el plazo de atención en 6 meses.

CONTIENE firmadigital Ley Nº8454
“Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita”

Recomendación 5:

Robert Picado Mora y Geiner Gamboa Otárola: Pedimos un ajuste en el plazo de la recomendación, dado que estimamos que 9 meses es lo mínimo para desarrollar lo solicitado.

Leonardo Díaz Porras: Acepta la observación y establece el plazo de atención en 9 meses.

Recomendación 6:

Robert Picado Mora: Yo podría entender que se plantee un plan de capacitación interno, pero mientras no se resuelva el tema de los recursos externos, considero que no es viable. La verdad es que no tengo gobernanza sobre el personal externo; no tiene sentido que yo asuma la responsabilidad de liderar un plan de capacitación si no tengo autoridad sobre esos recursos.

Si se decide avanzar en esa línea, entonces la capacitación debería dirigirse a los gerentes responsables. Mientras los recursos no estén bajo mi supervisión directa, no me corresponde capacitar a personal que no pertenece formalmente a TIC. Así es como lo veo.

Oscar Mena Granados: Aclara que lo solicitado es un plan orientado a fortalecer el conocimiento general, tanto en su estado actual como en función de las necesidades futuras. Señala que dicho plan puede incluir diversas estrategias, como videoconferencias, campañas de concientización y otras acciones que apoyen la cultura de cambio y, al mismo tiempo, promuevan la toma de conciencia sobre la evolución de habilidades que se requiere impulsar.

Geiner Gamboa Otárola: Sí, bueno, mucho de lo que iba a comentar ya se mencionó, pero quisiera que no perdamos de vista lo siguiente: cuando yo entrego un servidor, ya sea en la nube o local, lo importante es que el usuario lo reciba y pueda operarlo, porque la funcionalidad es la misma.

Desde la perspectiva del CGI, no es necesario tener un conocimiento profundo sobre si el servidor está en la nube o en sitio, porque lo que se entrega es un entorno funcional para su uso.

El conocimiento técnico que ya posee el CGI le permite gestionar estos entornos, independientemente de dónde estén alojados.

Estamos de acuerdo en que sí se requiere una pequeña inducción o guía para conocer las particularidades del ambiente en la nube, pero no es necesario reaprender a usar servidores o aplicaciones, ya que eso es parte de sus competencias actuales.

Leonardo Díaz Porras: Solo para reforzar la idea, don Robert: no perdamos de vista que la recomendación se traduce en un plan de acción, y ese plan es lo que ustedes van a entregar a la Auditoría. Ustedes son quienes definen el contenido y el alcance de ese plan.

En cuanto al personal local, entiendo perfectamente que cada unidad tiene su propia jerarquía y jefaturas. Por lo tanto, ustedes pueden establecer en el plan de acción que la actualización o reforzamiento del conocimiento se gestione mediante una guía, como bien lo mencionó Geiner anteriormente, que se entregue cada vez que se proporciona un servicio en la nube.

En resumen, la forma en que se aborde la actualización de conocimientos queda a su análisis: si consideran que es necesario un proceso más formal de capacitación para el nivel central o para el personal de TIC, lo pueden incorporar. Pero para el nivel local, basta con definir la estrategia que consideren adecuada, como una guía o cualquier otro mecanismo que cumpla con ese objetivo.

CONTIENE firmadigital Ley Nº8454
"Garantiza la autoría e integridad de los documentos digitales y la equivalencia jurídica de la firma manuscrita"

Robert Picado: Entiendo, estoy de acuerdo con la recomendación.

En relación con las recomendaciones 3, 4 y 7, no se presentaron observaciones.

En ese sentido, las observaciones recibidas fueron debidamente analizadas y valoradas por la Auditoría Interna, y han sido incorporadas en el informe correspondiente, según su pertinencia.

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Firmado digitalmente por OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Fecha: 2025.05.09 13:54:45 -06'00'

Lic. Oscar Mena Granados
Asistente de Auditoría

LEONARDO FABIO DIAZ PORRAS (FIRMA)
Firmado digitalmente por LEONARDO FABIO DIAZ PORRAS (FIRMA)
Fecha: 2025.05.14 10:28:48 -06'00'

Lic. Leonardo Fabio Díaz Porras, jefe a.i.
Área Tecnologías de Información y Comunicaciones

OSC/RJS/LDP/OMG/ayms