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

AS-AATIC-177-2022
23 de agosto de 2022

Doctora
María Eugenia Villalta Bonilla, gerente a.i.
GERENCIA GENERAL-1100

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

Estimadas señoras:

ASUNTO: Oficio de Asesoría sobre la gestión de servicios de computación en la nube como mecanismo de contingencia.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo del Área de Tecnologías de Información y Comunicaciones de esta Auditoria, para el período 2022, y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se emite la siguiente asesoría respecto a la gestión de la tecnología denominada Computación en la nube entre los mecanismos de contingencia Institucional.

Aspectos Generales

El 21 de abril del 2022, la Caja Costarricense de Seguro Social (CCSS) recibió un ataque cibernético dirigido al Portal de Recursos Humanos, lo cual ocasionó que se deshabilitara el acceso a esa plataforma tecnológica durante 15 días aproximadamente, con el objetivo de verificar si se logró el ingreso por parte de los atacantes o si hubo extracción de información sensible.

Posteriormente, el 31 de mayo de 2022, se detectó otro ciberataque, obligando a la Institución a deshabilitar la Infraestructura Tecnológica que soporta los diversos sistemas de informáticos, bases de datos y servicio de internet utilizados para la prestación de servicios a los usuarios en el territorio nacional.

El 1 de junio de 2022, a través de conferencia de prensa a medios nacionales, el Dr. Álvaro Ramos Chaves, presidente ejecutivo de la Institución, indicó lo siguiente:

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

Ante esta situación, esta Auditoría considera importante valorar diversas alternativas para garantizar continuidad de negocio y ciberseguridad ante posibles ataques de esta índole, entre las cuales se puede mencionar la implementación de la modalidad denominada computación en la nube, siendo que es una de las tendencias mundiales en la materia.

Computación en la nube

El Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST) define la Computación en la nube como un modelo para habilitar el acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción con el proveedor de servicios[1].

Tipos de nube informática

De forma general, existen tres tipos de nube informática definidas para satisfacer las diversas necesidades o requerimientos de las organizaciones, las cuales se describen a continuación:

- **Nube pública:** Consiste en la prestación de servicios informáticos e infraestructura externa a las empresas mediante el uso de internet público, se encuentran disponibles de forma gratuita y en su versión de pago, además, se utiliza a nivel general por diversas organizaciones y los proveedores de la nube se encargan de la administración y mantenimiento del hardware y software.

- **Nube Privada:** Es el conjunto de recursos computacionales configurados por demanda en el interior de una nube pública de un proveedor externo solo para un grupo de usuarios y no al público en general, ofrecen un nivel más alto de seguridad y privacidad con firewalls de la compañía y hospedaje interno, limitando así el acceso a los datos por los proveedores externos. La administración y los costos asociados a la nube privada se asumen por las empresas usuarias

- **Nube Híbrida:** Combina un centro de datos local (nube privada) con las facilidades que ofrece la nube pública, permitiendo a las empresas escalar o reducir verticalmente su capacidad de forma inmediata, controlar el exceso de demanda de servicios informáticos, evitar el tiempo y costo de adquirir, instalar y mantener servidores según sus necesidades actuales y futuras.

Modelos de servicio de computación en la nube

La computación en la nube permite a las organizaciones la opción de adquirir servicios escalables bajo la figura “as a Services”, donde se pueden adquirir facilidades tecnológicas sin tener que contemplar los costos de adquisición, administración, mantenimientos y actualización de un centro de datos propio.

[1] The NIST Definition of Cloud Computing | NIST

A continuación, se describen los modelos fundamentales de computación en la nube:

- **Software como Servicio (SaaS):** Servicios brindado por un proveedor de la nube que contempla la infraestructura y las aplicaciones que requieren los clientes mediante un modelo de pago de uso, lo cual implica que la institución o empresa utilizará los servicios y asumirá solamente el costo por su utilización. Además, la información gestionada a través de este modelo de servicio será almacenada en la plataforma del proveedor de la nube.

- **Infraestructura como Servicio (IaaS):** En este modelo de servicio de la nube, el proveedor aloja los componentes de infraestructura que normalmente se almacenan en centros de datos propios de una empresa u organización, entre los servicios que se ofrecen bajo esta modalidad se pueden encontrar, hardware de servidores y redes, servicios de virtualización, soluciones en la nube híbrida y servicios de almacenamiento.

- **Plataforma como Servicio (PaaS):** Este modelo de servicio en la nube es de pago según demanda y le provee a las empresas una infraestructura más específica de hardware y software para el desarrollo de aplicaciones para usuarios finales. Adicionalmente, los proveedores ofrecen servicios de alojamientos de sistemas operativos y servicios de middleware que los desarrolladores necesitan para crear y ejecutar aplicaciones.

Plan de contingencia en la nube o Cloud Based Disaster Recovery (CBDR).

La Recuperación de Desastres basado en la Nube (CBDR) ayuda rápidamente a las organizaciones a recuperar sus servicios críticos y proveerles acceso remoto de los sistemas ubicados en un ambiente virtual seguro posterior a la materialización de un riesgo que afecten los servicios que se brindan a través de las tecnologías de información y comunicaciones.

Así las cosas, la forma de operar del CBDR consiste en implementar de manera integral todo lo que se encuentra en el servidor afectado (sistema operativo, aplicaciones, aplicación de parches, datos) en un solo servidor virtual o paquete de software a través del proceso de copiado o replicación, caso contrario a la gestión que se debe llevar a cabo en una infraestructura tecnológica local donde se debe volver a cargar el sistema operativo, las aplicación y posteriormente realizar la última actualización de parchado de los componentes tecnológicos.

Observaciones

Esta Auditoría considera que, desde la perspectiva de la continuidad del negocio y el fortalecimiento de la ciberseguridad, es necesario se valore la factibilidad y conveniencia de considerarse necesario, la implementación y aprovechamiento de nuevas tecnologías entre las cuales se encuentra la computación en la nube en instituciones como la CCSS, máxime al dimensionar los efectos del ciberataque suscitado en los últimos meses. Lo anterior fundamentado en la naturaleza de este modelo en cuanto al almacenamiento y procesamiento informático de sistemas y servicios tecnológicos.

Aunado a lo anterior, es importante contemplar los beneficios que esta modalidad otorga en otros campos no asociados a la ciberseguridad, tal como interrupciones causadas por desastres naturales y demás riesgos que podrían afectar la integridad, confidencialidad y calidad de la información institucional.

Por lo tanto, esta Auditoria en su rol de asesoría, hace de conocimiento las siguientes observaciones, con el objetivo de que sean valoradas dentro de las acciones ejecutadas para el análisis de implementación, uso y proyección de tecnologías de computación en la nube, en la operación cotidiana de la infraestructura institucional y en apoyo a la continuidad de servicios, sin obviar los procedimientos y directrices establecidos en la normativa aplicable en el sector público y a nivel de la CCSS:

a) Definición de un marco de gobierno de la nube que brinde el direccionamiento Institucional para el cumplimiento de los objetivos estratégicos y metas acordados, toma de decisiones fundamentadas en aspectos como: la valoración de los riesgos inherentes a la utilización de esa solución tecnológica, costos de operación y proyección de inversiones.

b) Elaboración de un modelo de riesgos para determinar el apetito al riesgo del negocio respecto al uso de la nube informática, el cual contemple al menos los dominios de agilidad para satisfacer necesidades futuras imprevistas, disponibilidad ante interrupciones del servicio y pérdida de datos, seguridad de la información, cambios en el modelo del negocio del proveedor de la nube, incumplimiento de requisitos técnico-legales sobre el tratamiento y protección de los datos sensibles.

c) Análisis de los aspectos señalados en el oficio GA-DJ-00212-2021, respecto al criterio emitido por la Dirección Jurídica sobre el uso de la nube computacional basado en el análisis de diversos criterios técnicos y en apego a lo establecido en el marco normativo aplicable vinculado con la protección de las personas frente al tratamiento de los datos personales, donde se cita textualmente lo siguiente:

"Con sustento en todo lo expuesto, desde la perspectiva jurídica, resulta viable que la Administración activa, valore la posibilidad de aprovechar las bondades que ofrece los servicios en la nube, máxime que, como bien se indicó en el criterio técnico vertido mediante oficio GG-DTIC-5710-2020, "la nube" ofrece un potencial enorme para distintos servicios tecnológicos, algunos de los cuales ya están disponibles en la CCSS. Con la advertencia de que, todas las decisiones administrativas que se tomen deberán estar sustentadas en criterios técnicos calificados de todo orden (administrativos, financieros, contables, legales, de control de riesgos, entre otros) y apegadas a las disposiciones contenidas en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y su Reglamento."

d) Establecimiento de procesos que permitan a la CCSS supervisar la implementación y cumplimiento del marco normativo aplicable por parte del proveedor en temas asociados a la protección y tratamiento de los datos almacenados, definición de acuerdos de confidencialidad, según el servicio adquirido y asegurar que el negocio tome decisiones basadas en los estudios o análisis técnicos que considere pertinentes previos al uso de esa tecnología.

e) Elaboración de una estrategia sobre la implementación de servicios que provee la nube informática que permita a la Institución disponer de mecanismos de contingencia, considerando al menos los siguientes aspectos:

   i. Necesidades reales de la institución respecto a los servicios que ofrecen los proveedores tales como: SaaS, PaaS, IaaS, entre otros, lo anterior en aras de constatar su aprovechamiento óptimo de la inversión efectuada.

ii. Análisis de los datos a almacenar según el tipo de nube informática, lo anterior con el objetivo de apoyar la toma de decisiones sobre los mecanismos de seguridad a implementar que permitan salvaguardar su confidencialidad e integridad, la minimización de riesgos vinculados con la pérdida, robo, extravío o uso ilegal de ese activo Institucional.

iii. Análisis de factibilidad para determinar los beneficios, costos y riesgos de la adquisición y uso de las bondades que ofrece la nube informática para la CCSS en comparación con otras tecnologías y las diversas opciones de proveedores que se encuentran en el mercado actualmente, lo anterior para determinar la opción a seleccionar de acuerdo con las necesidades institucionales.

iv. Determinar el enfoque de la estrategia que permita flexibilidad entre las necesidades actuales de la Institución respecto a los sistemas de información propiedad de la CCSS y las innovaciones que se requieran a futuro para automatizar procesos del negocio.

v. Plan de transición de los servicios brindados actualmente a la nube informática, donde se tenga claridad sobre los recursos operativos requeridos, cronograma de actividades, cantidad y tipo de software y hardware disponible para el alojamiento en esa solución tecnológica considerando sus características técnicas, compatibilidad y el rendimiento esperado de las aplicaciones que se alojaran en esa plataforma.

vi. Elaboración de proyecciones sobre aspectos de escalabilidad, integración, crecimiento y reemplazo del software y hardware contemplando el plan de reemplazo y capacidad tecnológico actual, lo anterior con el objetivo de minimizar posibles vulnerabilidades de seguridad y analizar los diferentes escenarios respecto a la adquisición de tecnologías en el futuro y su compatibilidad.

f) Establecer el modelo de seguridad compartida que involucre al proveedor del servicio de la nube informática y a los clientes, determinando así, aspectos asociados a los roles y responsabilidades sobre la utilización de los servicios adquiridos, configuraciones de seguridad de los componentes que van a interactuar en ese ambiente y acuerdos de servicio.

g) Analizar la redundancia de los servicios ofrecidos por los proveedores de la nube informática, lo anterior con el objetivo de constatar la continuidad de las actividades que dependan de las tecnologías alojadas en esa solución ante una falla o imprevisto de los servicios contratados y revisar las leyes o normativa respecto a la protección y tratamiento de los datos sensibles, según el lugar donde se almacene la información en caso de alguna eventualidad.

h) Revisar el plan de capacitación Institucional y los temas vinculados con la formación de personal calificado sobre el uso, beneficios y riesgos de los servicios que ofrece la nube informática, minimizar la materialización de riesgos vinculadas, desconocimiento de ese tipo de tecnologías, configuraciones incorrectas y/o utilizaciones indebidas que podrían ser aprovechadas por los cibercriminales para infiltrarse en la infraestructura y perpetrar ciberataques.

i) Analizar las diversas soluciones y tipos de cifrado requeridos por la Institución para proteger la información gestionada durante su recolección, consulta y almacenamiento en la nube, lo anterior en aras de minimizar los riesgos vinculados con la intercepción de datos sensible por parte de los cibercriminales. Además, es relevante considerar las recomendaciones de seguridad respecto a las claves de cifrado y su almacenamiento de forma segura.

j) Establecimiento de procesos que sirvan de guía a los usuarios internos de la CCSS para la solicitud, configuración y suspensión de servicios en la nube, lo anterior con el objetivo de lograr una estandarización, fortalecimiento de las actividades sustantivas de control interno y minimizar riesgos vinculados con el uso indebido de los recursos adquiridos.

k) Elaboración de una estrategia de salida de la nube que brinde la orientación sobre el actuar Institucional ante la suspensión de los servicios adquiridos sin ocasionar afectación en las actividades sustantivas del negocio.

Consideraciones normativas

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en los apartados III. Planificación tecnológica institucional y IV. Gestión de riesgos tecnológicos, se indica lo siguiente:

"III. PLANIFICACIÓN TECNOLÓGICA INSTITUCIONAL

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.

La Unidad de TI debe disponer de un plan de infraestructura e inversiones que permita proyectar los requerimientos de licenciamiento, mantenimiento de infraestructura tecnológica (preventiva, por obsolescencia, mejora), adquisición de nuevos recursos tecnológicos, basados en la línea estratégica institucional establecida

La Unidad de TI debe disponer de un programa de iniciativas institucionales que pueden ser habilitadas a través de la incorporación de recursos y servicios tecnológicos, respaldados debidamente por la valoración de la factibilidad y entrega de valor respectivos.

La Unidad de TI debe desarrollar la planificación anual operativa que oriente las acciones para asegurar la mantenibilidad y disponibilidad de los recursos tecnológicos, la incorporación de nuevas facilidades (a través de proyectos) y el presupuesto asociado a las actividades y tareas, debidamente alineadas con los objetivos estratégicos establecidos por la institución.

La entidad debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando
el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable

IV. GESTIÓN DE RIESGO TECNOLÓGICO

La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."

Adicionalmente, esas Normas técnicas, en el inciso VIII. Contratación y adquisiciones de bienes y servicios tecnológicos, señala lo siguiente:

VIII. CONTRATACIÓN Y ADQUISICIONES DE BIENES Y SERVICIOS TECNOLÓGICOS

La institución debe disponer de prácticas formales para establecer los requerimientos de contratación y adquisición de bienes, consultorías y servicios a proveedores externos, cuyo giro de negocio sea orientado al ámbito tecnológico, de forma tal que apoye el desarrollo de iniciativas y mejoras de la infraestructura tecnológica, sistemas de información, seguridad de la información, ciberseguridad y otros relacionados de acuerdo con las necesidades y oportunidades visualizadas al nivel institucional. El modelo debe permitir establecer objetivamente al nivel operativo, técnico, legal y tecnológico entre otros, los términos de referencia, los parámetros de valoración del perfil del proveedor y su oferta para realizar la selección adecuada.

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.

Esas mismas Normas técnicas, en los apartados XI. Seguridad y ciberseguridad, XII. Administración Infraestructura tecnológica y XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, señala:

*"**XI. SEGURIDAD Y CIBERSEGURIDAD***

La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información (…)"

XII. ADMINISTRACIÓN INFRAESTRUCTURA TECNOLÓGICA

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.

(…) XIII. CONTINUIDAD Y DISPONIBILIDAD OPERATIVA DE LOS SERVICIOS TECNOLÓGICOS

La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estratega viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.

La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.

La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."

La Directriz No 46-H-MICITT, estípula en el artículo 1°, lo siguiente:

> *"Artículo 1°- A partir de la publicación de esta directriz las instituciones del sector público privilegiarán, cuando sea posible y conveniente, la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura. Esto aplica para equipos, licencias y sistemas informáticos, servidores de hospedaje de páginas Web, servidores de aplicaciones, correo electrónico, muros de fuego, sistemas operativos, sistemas ofimáticos, bases de datos u otras tecnologías informáticas ya sea para el usuario final o para el centro de datos en sí, o cualquier otro tipo de desarrollo tecnológico. Se busca con esta directriz facilitar el acceso a plataformas tecnológicas en concordancia con los planes de modernización del Estado y garantizar su disponibilidad independientemente de ubicación física, respetando criterios de uso racional de recursos públicos."*

CONSIDERACION FINAL

La tendencia de las inversiones en soluciones vinculadas con Cloud Computing, ha venido aumentando en las empresas y organizaciones a nivel mundial a través de los años y la CCSS no es la excepción, por lo tanto, resulta importante se efectúe una gestión de la computación en la nube que logre minimizar riesgos de vulnerabilidades de ciberseguridad que afecten la confidencialidad, integridad y calidad de los datos sensibles de los usuarios o comprometer la continuidad de las actividades brindadas a través esas tecnologías de información y comunicaciones.

Al respecto, según lo señalado por diversas empresas reconocidas internacionalmente, la adopción de la computación en la nube, les ha permitido avanzar en diferentes ámbitos del negocio, mejorar el rendimiento de las operaciones, la optimización de recursos y la obtención de resultados minimizando costos y tiempo, un ejemplo de ello es la compañía General Electric, quien implementó los servicios en la nube durante el 2014 y para el 2017 logró redireccionar al personal que brindaba mantenimiento al centro de datos local para la gestión de tareas de innovación.

Así mismo, según el informe Hybrid Cloud Report 2021 de la empresa NTT Data, el 93,7% de las empresas encuestadas consideró la nube un componente fundamental para gestionar las necesidades inmediatas del negocio producto de la pandemia.

En virtud de lo expuesto anterior, tener presentes aspectos asociados a la definición de estrategias de implementación y salida de la nube que sean flexibles a los cambios, la actualización de las necesidades futuras podría llegar a ser la diferencia en el aprovechamiento de ese tipo de tecnologías y los beneficios obtenidos para la Institución.

Por otra parte, no se pueden descuidar la ejecución de acciones para el resguardo de la integridad y confidencialidad de los datos gestionados a través de la computación en la nube, que contribuyan en el fortalecimiento de la ciberseguridad tales como: el establecimiento del modelo de seguridad compartida entre el proveedor y el cliente para tener claridad respecto a los roles y responsabilidades de las partes involucradas, implementación de soluciones de cifrado de datos y la capacitación del personal que va a configurar y utilizar los servicios adquiridos.

Además, es importante considerar lo esbozado en el documento GA-DJ-00212-2021, en el cual la Dirección Jurídica hace referencia a la valoración de estudios y consideraciones técnicas y legales previo a la toma de decisiones por parte del negocio, respecto a la utilización de los servicios brindados por tecnologías como la computación en la nube.

Así las cosas, este Órgano de Fiscalización y Control en su rol de asesor, informa sobre los aspectos esbozados en el presente oficio, con el objetivo de que sean revisadas y analizadas en forma conjunta con las instancias institucionales que estime pertinente, a fin de planificar y ejecutar una estrategia orientada a la valoración de computación en la nube entre las alternativas para el procesamiento, almacenamiento y respaldo de información de sistemas y servicios, lo anterior considerando aspectos de ciberseguridad y continuidad de los servicios institucionales brindados ante cualquier incidente sin descuidar posibles riesgos asociados a la seguridad de la información gestionada por la CCSS.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.08.24 17:27:01 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/GMP/lbc

C. Máster Esteban Zúñiga Chacón, jefe, Centro de Gestión Informática, Gerencia Médica- 2901.
Licenciado Alexander Solís Vargas, jefe, Centro de Gestión Informática, Gerencia Financiera-1103.
Máster Giselle Tenorio Chacón, jefe, Centro de Gestión Informática, Gerencia Administrativa-1104.
Ingeniero Roy Ovares Valerio, jefe, Centro de Gestión Informática, Gerencia de Logística-1106.
Licenciado Giovanni Campos Alvarado, jefe, Centro de Gestión Informática Gerencia de Infraestructura y Tecnologías- 1107.
Licenciado Marco González Jiménez, jefe, Centro de Gestión Informática, Gerencia de Pensiones- 9108
Auditoría