INFORME N.° **DFOE-SOC-IF-00024-2019**
20 de diciembre, 2019

INFORME DE LA AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LOS CONTROLES TECNOLÓGICOS EN EL SISTEMA DE RECAUDACIÓN DE LA CCSS

2019

Contraloría General de la República, Costa Rica
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización de Servicios Sociales

CONTENIDO

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría de carácter especial tuvo como objetivo determinar si los controles tecnológicos implementados en el sistema de recaudación de la Caja Costarricense del Seguro Social (CCSS) ofrecen una garantía razonable de la seguridad de la información almacenada en sus bases de datos. En el período comprendido del 1 de enero de 2015 al 31 de diciembre de 2018, el cual se amplió cuando se consideró necesario. Específicamente, se valoraron aspectos de Gestión de la Seguridad de la Información del Sistema Centralizado de Recaudación (SICERE), relativos a riesgos en la continuidad de los servicios de recaudación; gestión de permisos a usuarios para el acceso al SICERE y sistemas conexos; controles tecnológicos; y análisis de "Procesos Diferidos" en relación con la operación del sistema. Además, de aspectos que tienen efecto en el desempeño del sistema, relativos a gestión y gobierno de tecnologías de información en la CCSS.

¿POR QUÉ ES IMPORTANTE?

El SICERE administra a los contribuyentes de la CCSS, de manera que por medio de este sistema se capta la mayoría de sus ingresos, por lo que se convierte en factor clave para la recaudación y financiamiento de la entidad.

La CCSS cuenta con un porcentaje de cobertura contributiva del Seguro de Salud respecto a la población total para el año 2018 en un 76,8%, manteniendo la tendencia creciente especialmente en las categorías de aseguramiento directo de asalariados, cuenta propia, y pensionados de IVM; para un total de 1.744.838 trabajadores.

En cuanto a los ingresos recibidos por medio de la gestión de recaudación para el periodo 2018, se percibió ¢2.763.668,6 millones en el Seguro de Salud; ¢1.312.202,2 millones en el Régimen de Invalidez, Vejez y Muerte y ¢161.423,6 en el Régimen no Contributivo de Pensiones.

¿QUÉ ENCONTRAMOS?

Una vez concluida la presente auditoría, esta Contraloría General determinó que los controles tecnológicos implementados por la CCSS para la seguridad de la información del SICERE, presentan debilidades en aspectos tales como, riesgos en la continuidad de los servicios relacionados con la recaudación en la CCSS, debilidades en la gestión de permisos a usuarios para el acceso al SICERE y sistemas conexos, insuficiencia de los controles tecnológicos, y riesgo en el desempeño del SICERE por el crecimiento de los "Procesos Diferidos".

Así las cosas, en cuanto a la continuidad de los servicios, este Órgano Contralor, determinó riesgos en la operación del SICERE de la CCSS, debido a que la institución no ha definido planes de continuidad de negocio para este servicio. Servicio de especial relevancia, y que involucra a todos los asegurados, entidades recaudadoras asociadas a la CCSS, las operadoras de pensiones y la función de validación de derechos del sistema de Expediente Digital Único en Salud (EDUS). En este contexto, se encontró que no se cuenta con planes de contingencia informática, atención de emergencias, sucesión y recuperación de desastres, actualizados y aprobados que garanticen la operación continua del servicio.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Por otra parte, respecto de la gestión de permisos a usuarios este Órgano Contralor determinó que existe un riesgo en el manejo de la información contenida en el SICERE y sistemas conexos, puesto que, se evidenció un retraso en los ajustes a los privilegios de acceso asignados por roles, a funcionarios que cambian su condición laboral o dejan de laborar para la institución, por cuanto continúan activas credenciales que deberían ser canceladas o cambiadas en forma inmediata. A manera de ejemplo, se detectaron 119 funcionarios que poseen roles activos en SICERE y sistemas conexos, los cuales de acuerdo a su definición de funciones en el "Manual Descriptivo de Puestos" de la CCSS no debe tener asignado ningún perfil.

En cuanto a la insuficiencia de los controles tecnológicos, se detectó que en relación con la aplicación de la Oficina Virtual - Módulo Autogestión Planilla en Línea -, módulo que es utilizado por los patronos mes a mes, se presentan limitaciones en materia de aseguramiento, con respecto a la información que el patrono puede digitar. A mayor abundamiento, se determinaron situaciones como las siguientes: el patrono incluye ocupaciones que no corresponden a un tipo de planilla específica, se reportan salarios altos de trabajadores, en algunos casos de ¢8,000,000 y hasta ¢12,000,000, vinculados, por ejemplo, con mujeres incapacitadas por maternidad, se realiza una inscripción patronal, sin valorar su condición de trabajador independiente. Además, el sistema permite el cierre de una planilla aunque tenga trabajadores activos laboralmente.

Por su parte, en lo que respecta, al riesgo en el desempeño del SICERE por el crecimiento de los "Procesos Diferidos" (procesos que se ejecutan fuera de horario normal de atención), se encontró que del período julio 2016 a setiembre 2019, estos procesos han crecido en un 43%. Así las cosas, a setiembre de 2019 se presentan 234 procesos diferidos, en cuyo caso, se resalta el riesgo operativo del SICERE por la existencia de esta gran cantidad de procesamientos diferidos.

Otros aspectos desarrollados con efectos en el desempeño del SICERE encontrados con la presente auditoría, y vinculados con la gestión y gobierno de tecnologías de información en la CCSS, se relacionan con la ausencia de formalización del funcionamiento del Consejo Tecnológico y de la Unidad Operativa para la implementación de la Agenda Digital Institucional. Dentro de este contexto, esta Contraloría General, determinó la ausencia de políticas, lineamientos u otros marcos normativos formalmente aprobados y divulgados dentro de la CCSS, en torno al funcionamiento de este Consejo.

Además, se evidencia falta de definición de la estructura organizativa de la Dirección de Tecnologías de Información y Comunicación (DTIC), y un rezago en el uso de la infraestructura tecnológica y datos del SICERE para la toma de decisiones. A mayor abundamiento en cuanto a este último punto, se determinó que si bien es cierto el SICERE contiene información histórica y actual, la cual es altamente valiosa para la toma de decisiones financiera y operativa de la CCSS, y que además, se han realizado esfuerzos importantes en la adquisición de servicios profesionales así como licenciamiento para la conformación de herramientas e infraestructura que le permite manejar una suite de tecnologías en la implementación de soluciones BI, Big Data, analítica predictiva. Dichas herramientas no son utilizadas por las autoridades de la CCSS para la toma de decisiones. Dentro de este contexto, según encuesta realizada por este Órgano Contralor se desprende que el 85.2% de las jefaturas, directores consultados, indica no usar alguna solución de inteligencia de negocios para la toma de decisiones.

¿QUÉ SIGUE?

Dados los hallazgos de la presente auditoría se giran una serie de disposiciones a las autoridades de la CCSS, dentro de las cuales caben destacar: la elaboración, aprobación e implementación de un plan de continuidad servicios para el SICERE, definición e implementación de acciones específicas que permitan llevar a cabo una revisión completa de

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

todos los roles y perfiles actuales con el propósito de corregir las debilidades sobre estos accesos de los funcionarios al SICERE y sistemas conexos. Además, elaborar, divulgar e implementar mecanismos de control que permitan asegurar, de forma permanente, los niveles de acceso de los funcionarios a los sistemas de información, con la debida rectoría por parte de la Dirección SICERE.

A su vez, elaborar e implementar mecanismos de control tecnológicos que garanticen el cumplimiento de la normativa y las reglas de negocio en la aplicación Oficina Virtual - Módulo Autogestión Planilla en Línea, elaborar un estudio que permita identificar cada uno de los "procesos diferidos" que pueden ser reestructurados y convertidos a procesos en línea, con el propósito de contar con información actualizada y minimizar los riesgos del procesamiento fuera de línea.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN DE SERVICIOS SOCIALES

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LOS CONTROLES TECNOLÓGICOS EN EL SISTEMA DE RECAUDACIÓN DE LA CCSS

1. Introducción

ORIGEN DE LA AUDITORÍA

1.1. El gobierno y la gestión de las tecnologías de información en una institución permite el cumplimiento de sus objetivos institucionales y la adecuada toma de decisiones, mediante el aseguramiento razonable de la confiabilidad, integridad y disponibilidad de la información que respalda sus funciones sustantivas.

1.2. Por lo tanto, cabe recalcar que la Caja Costarricense de Seguro Social (CCSS), mediante el *Sistema Centralizado de Recaudación (SICERE)* administra a los contribuyentes de la seguridad social, por lo que se convierte en factor clave para la recaudación de los ingresos de la entidad, y es relevante para la gestión del Régimen Obligatorio de Pensiones y el Fondo de Capitalización Laboral el cual distribuye entre todas las operadoras de pensiones.

1.3. En cuanto a los ingresos recibidos por medio de la gestión de recaudación para el periodo 2018, se percibió ¢2.763.668,6 millones en el Seguro de Salud; ¢1.312.202,2 millones en el Régimen de Invalidez, Vejez y Muerte y ¢161.423,6 en el Régimen no Contributivo de Pensiones.

1.4. Cabe indicar, que la auditoría se ejecutó en cumplimiento del Plan Anual Operativo de la DFOE con fundamento en las competencias que le son conferidas en los artículos 183 y 184 de la Constitución Política; y 12, 17 y 21 de su Ley Orgánica, N° 7428.

OBJETIVOS

1.5. Determinar si los controles tecnológicos implementados en el sistema de recaudación de la CCSS ofrecen una garantía razonable de la seguridad de la información almacenada en sus bases de datos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

ALCANCE

1.6. Se indagó acerca de los controles tecnológicos del SICERE y sistemas conexos que intervienen en el proceso de recaudación de la CCSS, valorando aspectos de gestión que provean el aseguramiento de la continuidad de los servicios, permisos a usuarios, así como el análisis de "Procesos Diferidos" en relación con la operación del sistema y que puedan tener efecto en el desempeño del sistema. Además, de aspectos que tienen efecto en el desempeño del sistema, relativos a gestión y gobierno de tecnologías de información en la CCSS.

1.7. El período de análisis comprende desde el 01 de enero de 2015 hasta el 31 de diciembre de 2018, ampliándose cuando se considere necesario

CRITERIOS DE AUDITORÍA

1.8. Los criterios de auditoría fueron comunicados formalmente a Roberto Cervantes Barrantes en su calidad de Gerente General mediante el oficio N° DFOE-SOC-1073 del 24 de octubre de 2019.

METODOLOGÍA APLICADA

1.9. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE. Los procedimientos de auditoría ejecutados consideraron el análisis de la información suministrada en entrevistas y consultas escritas por funcionarios de la CCSS.

1.10. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas a funcionarios de la CCSS, así como las respuestas a las consultas planteadas por escrito ante diferentes funcionarios de esa institución.

1.11. En cuanto a la medición de la información contenida en el SICERE y el Sistema Integral de Gestión de Inspección (SIGI) se efectuó una encuesta electrónica desde la plataforma de Google a 1.243 funcionarios; la cual fue segmentada por niveles (operativo, mandos medios). El uso de la encuesta tuvo como finalidad conocer la opinión sobre calidad de la información (utilidad, oportunidad y confiabilidad), y flexibilidad, la cual, es utilizada para la toma de decisiones.

1.12. Finalmente se desarrolló el análisis de información sobre los datos extraídos directamente de la base de datos referente a los perfiles, usuarios, centros de salud, entre otros.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.13. Se obtuvo la colaboración de dos funcionarios de la auditoría interna de la CCSS, mediante un acuerdo entre la Contraloría General de la República y la institución auditada, esto fue a tiempo completo durante el periodo que abarcó la presente auditoria, pasando a ser estos funcionarios parte del equipo de trabajo responsable de los procedimientos y hallazgos encontrados.

LIMITACIONES QUE AFECTARON LA EJECUCIÓN DE LA AUDITORÍA

1.14. Se presentó en el desarrollo de la auditoría, falta de oportunidad en el suministro de alguna información requerida, además de información que en algunos casos se

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

proporcionaba de manera incompleta, lo que generó atrasos en la realización de algunos procedimientos.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.15. La seguridad social, entendida como el conjunto de servicios de salud, asistencia social y previsión, es un tema que requiere atención y la CCSS como ente del Estado costarricense responsable del control y administración de los elementos relacionados con la recaudación y aseguramiento que conlleva el empleo remunerado permanente, así como el modelo de inserción de las personas en las estructuras laborales, determinando que la protección social sea ejercida por igual por todos y todas. El concepto de seguridad social en Costa Rica es un derecho y un objetivo de cobertura nacional.

1.16. Dada esta responsabilidad es que la CCSS adquiere y desarrolla como solución el SICERE, herramienta tecnológica que le permite automatizar la gestión para los procesos de Facturación, Recaudación y Distribución de las aportaciones a la Seguridad Social, abarcando las de la Caja, el INA, IMAS, Asignaciones Familiares, Banco Popular, la gestión del régimen de Asegurados Voluntarios, Trabajador Independiente y lo referente al Régimen de Pensiones Complementarias y Fondo de Capitalización Laboral, constituidos en la Ley de Protección al Trabajador, todo ello bajo un único marco donde el principal objetivo es mejorar la atención al patrono, trabajador, asegurado voluntario y trabajador independiente.

1.17. Por tanto, actualmente el SICERE permite gestionar la información de los patronos físicos y jurídicos, así como trabajadores independientes y asegurados voluntarios. Adicionalmente, esta herramienta se integra con diferentes sistemas institucionales, tales como: Sistema Registro, Control y Pago de Incapacidades (RCPI), Sistema Integrado de Pagos (SIPA), Sistema Integrado de Pensiones (SIP), Sistema Institucional para la Gestión de Inspección (SIGI), entre otros, por ende, resulta de vital importancia no solo para la CCSS sino para el país su adecuada administración

1.18. Lo anterior de conformidad con lo dispuesto en el artículo 73 de la Constitución Política y el artículo 20 de su Ley Constitutiva, como ente encargado del gobierno y administración de los Seguros de Salud y de Invalidez, Vejez y Muerte, debe velar por el cumplimiento de las obligaciones obreras y patronales, así como de la efectiva recaudación del pago de las cuotas derivadas de las diferentes modalidades de aseguramiento.

1.19. Se sabe que la CCSS cuenta con un porcentaje de cobertura contributiva del Seguro de Salud respecto a la población total para el año 2018 en un estimado del 76,8%, manteniendo la tendencia creciente especialmente en las categorías de aseguramiento directo de asalariados, cuenta propia, y pensionados de IVM; para un total de 1.744.838 trabajadores.

1.20. En cuanto a los ingresos recibidos por medio de la gestión de recaudación para el periodo 2018, se percibió ¢2.763.668,6 millones en el Seguro de Salud; ¢1.312.202,2 millones en el Régimen de Invalidez, Vejez y Muerte y ¢161.423,6 en el Régimen no Contributivo de Pensiones.

1.21. Aunado a lo anterior, la CCSS con corte a octubre 2019 cuenta con más de 57.600 funcionarios, los cuales se encuentran distribuidos a lo largo del país entre sus 80 sucursales, 7 direcciones de redes integradas de prestación de servicios de salud, 104

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

sedes de salud, 521 EBAIS, 689 puestos de salud periódica y 7 gerencias (General, Financiera, Administrativa, Infraestructura y tecnología, Médica, Logística y Pensiones).

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.22. Mediante la Advertencia[1] que emite este Órgano Contralor a la Administración, sobre los riesgos identificados con el avance del Plan de Innovación, específicamente del programa "Implementación de un ERP", se realiza la habilitación del Modelo de Administración del Portafolio, así como priorizar el desarrollo de los requisitos previos definidos por la CCSS que corresponde los proyectos complementarios, el cual es el insumo de entregables al posible adjudicatario de la licitación[2] para el ERP.

SIGLAS

SIGLA	Significado
BI	Inteligencia de Negocios
CCSS	Caja Costarricense del Seguro Social
CGR	Contraloría General de la República
CGI	Centros de Gestión Informática
COBIT	Control Objectives for Information and related Tecnology
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DTIC	Dirección de Tecnologías de Informática y Comunicación
EBAIS	Equipo Básico de Atención Integral en Salud
EDUS	Expediente Digital Único en Salud
ERP	Sistemas de Planificación de Recursos Empresariales
IMAS	Instituto Mixto de Ayuda Social
INA	Instituto Nacional de Aprendizaje
IVM	Invalidez, Vejez y Muerte
LGCI	Ley General de Control Interno
RCPI	Sistema Registro, Control y Pago de Incapacidades
SICERE	Sistema Centralizado de Recaudación
SIP	Sistema Integrado de Pagos
SIPA	Sistema Integrado de Pensiones
TIC	Tecnologías de la Información y Comunicación

[1] CGR, Oficio Nro.13983 (DFOE-SOC-0945) del 18 de setiembre, 2019.
[2] Según se constata con el oficio GF-3103-2019, del 08 de julio del 2019.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2. Resultados

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Riesgo en la continuidad de los servicios relacionados con la recaudación de la CCSS

2.1. En cuanto a la importancia de mantener los servicios en operación constante, las Normas de Control Interno para el Sector Público (NCISP)3, apartado 5.9 Tecnologías de información, indican que "deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información.".

2.2. Además, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (NTGCTI)4, emitidas por la Contraloría General de la República, en su punto 1.4.7, establecen que "La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.".

2.3. Por último las buenas prácticas establecidas en el marco de trabajo de COBIT 5[5], en su proceso DSS04, indican que se debe "establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.".

2.4. También la práctica de gestión DSS04.02 (COBIT 5) amplía que el proceso de continuidad implica "evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.".

2.5. Este mismo proceso de COBIT 5, en su práctica de gestión DSS04.03 específica que este plan debe estar basado en una estrategia que documente los procedimientos y la información lista para el uso en caso de un incidente, para facilitar que la empresa continúe con sus actividades críticas.

2.6. Asimismo la práctica de gestión DSS04.04 (COBIT 5) establece la necesidad de "probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.".

[3] Emitidas por la Contraloría General de la República mediante Resolución R-CO-9-2009 del 26 de enero del 2009 (N-2-2009-CO-DFOE).
[4] Aprobadas mediante Resolución del Despacho de la Contralora General de la República nro. R-CO-26-2007 del 7 de junio de 2007.
[5] "COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa", ISACA, 2012.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.7. Por medio del estudio de auditoría realizado por este Órgano Contralor, se determinaron riesgos en la operación del SICERE de la CCSS, debido a que la institución no ha definido planes de continuidad de negocio para este servicio. Servicio de especial relevancia, y que involucra a todos los asegurados, entidades recaudadoras asociadas a la CCSS, las operadoras de pensiones y la función de validación de derechos del sistema de Expediente Digital Único en Salud (EDUS), entre otros.

2.8. Sobre esta temática las autoridades de la CCSS remitieron a esta Contraloría General un documento denominado "Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones ASCI-UCG-0RG-002" el cual fue aprobado y divulgado desde Mayo 2013, mismo que debe ser aplicado por las unidades programáticas de la institución, para atender de manera general las fallas que se puedan presentar a nivel de hardware así como el control de licencias de software. Basado en el documento supra indicado la DTIC crea el documento "PCGTIC-AST-001: Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones.".

2.9. No obstante, valorados dichos documentos, este Órgano Contralor determinó que dentro de estos no se hace referencia a la operación específica del SICERE.

2.10. A mayor abundamiento, sobre este particular, según la hoja de control de actualización del plan de contingencia informática recibido, se creó en el año 2014 y se volvió a actualizar hasta el año 2018. Este tipo de planes contiene información de toda la plataforma tecnológica y sus riesgos, todo ello, por su naturaleza, es de carácter altamente cambiante y esa frecuencia de actualizaciones resulta a toda luz insuficiente para el tipo de información que contiene y su nivel de criticidad para el negocio.

2.11. Asimismo, cabe mencionar que, en lo que respecta a dicho plan de contingencia informática, esta Contraloría General, determinó que se encuentra incompleto al no contar con las fechas de llenado y actualización de cada plantilla, tiempos máximos de interrupción y mantenimiento del plan. Por su parte, no existe documentación que consigne las pruebas necesarias para garantizar razonablemente su efectividad en caso de suceder eventos adversos a la operación de los sistemas.

2.12. Por último, el citado plan no incluye la recuperación de los servicios en caso de interrupciones y desastres, esto por no obedecer a parámetros objetivos de tiempos y puntos de recuperación que hayan sido definidos mediante un proceso de análisis de impacto de negocio. Dentro de este contexto, en lo que respecta al ámbito de la continuidad del servicio específicamente del SICERE, tampoco se cuenta con un Centro de Datos alterno que pueda ser utilizado en caso de una interrupción que amerite la suspensión del Centro de Datos Primario.

2.13. Dado a que la CCSS no cuenta con un plan para el tratamiento de eventos adversos, que le asegure razonablemente la continuidad de los servicios suplidos por el SICERE y sistemas conexos, que se apoye en la contingencia informática, además, no se cuenta con el manejo de incidentes ni la recuperación de desastres para los sistemas de recaudación.

2.14. El no contar con planes de continuidad de negocio, puede llevar a la institución a detener las operaciones básicas soportadas por el SICERE en tiempos prolongados, si se llega a presentar un evento mayor y no se cuenta con mecanismos para restaurar los servicios dentro de tiempos definidos y razonables, con las implicaciones que repercutirán en los diferentes sectores, en servicios que resultan fundamentales.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.15. De esta forma, si un asegurado se presenta a un Centro de Salud de la CCSS en el momento que exista una interrupción del servicio del SICERE, este no podrá ser atendido ya que para cumplir con el proceso de validación de derechos el sistema EDUS requiere hacer uso de información contenida en la base de datos del SICERE para verificar el estado y las condiciones del asegurado que le permitan indicar si cumple con la normativa de la institución para ser atendido sin incurrir en cobros infundados.

2.16. Asimismo, el SICERE es el medio por el cual se distribuye dinero a las operadoras de pensiones, servicio que también podría verse comprometido ante fallas de ese sistema, en este caso, montos que superan los ¢439.212,8 millones de colones anuales (datos suministrados por la administración al 2017).

Debilidades en la gestión de permisos a usuarios para el acceso al SICERE y sistemas conexos

2.17. Tal como lo establecen las NCISP en el inciso 5.8 Control de sistemas de información; "el jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.".

2.18. Además la norma 1.4 del Manual de Normas técnicas para la gestión y el control de las Tecnologías de Información (MNTGCTI), nro. R-CO-26-2007 del 7 de junio de 2007 establece que "la organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos: /... El control de acceso. /... Además debe establecer las medidas de seguridad relacionadas con: /... La terminación normal de contratos, su rescisión o resolución.".

2.19. También la norma 1.4.5 de ese mismo cuerpo normativo establece que "la organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: / a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. /… d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI. e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones. f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI.".

2.20. En cuanto a las sanas prácticas internacionales contenidas en el proceso DSS05, denominada "Gestionar los Servicios de Seguridad" del COBIT 5, señala la "necesidad de "proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad". Este proceso especifica que se deben llevar a cabo, entre otras, las siguientes actividades: "mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.".

2.21. También COBIT 5 menciona, en la práctica de gestión DSS06.03 (Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización) que se deben "gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quién los está manejando en su nombre". Para esta práctica de gestión, establece que se deben llevar a cabo, entre otras, las siguientes actividades: "asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas. Asignar derechos de acceso y privilegios sólo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto predefinidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio.".

2.22. Por último, la Norma ISO 27002 "Tecnologías de Información. Código de prácticas para la gestión de la seguridad de la información", también nos indica, en su aparte 8.3.3 que "los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información deberían ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia.".

2.23. Este Órgano Contralor determinó que existe un riesgo en el manejo de la información contenida en el SICERE y sistemas conexos, puesto que, se evidenció un retraso en los ajustes a los privilegios de acceso asignados por roles, a funcionarios que cambian su condición laboral o dejan de laborar para la institución, por cuanto continúan activas credenciales que deberían ser canceladas o cambiadas en forma inmediata. En cuyo caso, no se respeta el margen establecido en cuanto a esta materia, en el "Manual Sobre la Operativa de las Labores de Administración de Usuarios y Perfiles en el Sistema Centralizado de Recaudación6.".

2.24. Dentro de este contexto, este Órgano Contralor encontró que la CCSS cuenta con 31 exfuncionarios acogidos a la jubilación con roles activos en SICERE y sistemas conexos, de los cuales el promedio de días desde su jubilación hasta setiembre 2019 es de 240 días, y en tres casos exfuncionarios con más de 579 días de jubilados.

2.25. Asimismo, sobre los roles de las personas jubiladas se detectaron 14 perfiles activos distintos, de los cuales la mayoría tienen permisos de ingresar, modificar o eliminar información. Así las cosas, cabe destacar que, se encontró un usuario activo que corresponde a un exfuncionario que se jubiló hace 304 días, que mantiene un perfil del sistema de Facturación por Servicios Médicos, diseñado para jefaturas de validación de derechos.

[6] Aprobado y divulgado por la gerencia financiera el 03 de abril de 2014 (GF-22836-14).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.26. Por su parte, en cuanto a funcionarios activos de la CCSS, se detectaron 119 que poseen roles activos en SICERE y sistemas conexos, los cuales de acuerdo a su definición de funciones en el "Manual Descriptivo de Puestos" de la CCSS no debe tener asignado ningún perfil a dichos sistemas. Lo cual se puede ver en forma detallada en el siguiente cuadro:

Cuadro N°. 1

Caja Costarricense de Seguro Social

Funcionarios activos con puestos que no deben tener relación con los perfiles asignados, por puesto y cantidad de funcionarios

Puesto	Cantidad de funcionarios
Trab.Serv.Generales	61
Guarda	16
Bodeguero	13
Auxiliar de Nutrición	9
Mensajero	9
Chofer 1	6
Técnico en Mantenimiento 2	4
Chofer 2	1
Total	**119**

Fuente: Elaboración propia con los datos suministrados en DAGP-0952-2019 y DAP-883-2019

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.27. A su vez, esta Contraloría General determinó, la existencia de hasta cuatro funcionarios activos en una sucursal con perfil de "Jefe Sede Sucursal", perfil que según las especificaciones establecidas es asignado solamente a los jefes de sucursal, puesto que, dentro de sus atributos indica que "puede registrar, consultar y actualizar información de los casos. Puede generar reportes de gestión y rendimiento de la sucursal a su cargo". A mayor abundamiento, sobre este particular, se incluye el siguiente cuadro:

Cuadro N°. 2

Caja Costarricense de Seguro Social

Cantidad de funcionarios con perfil del SIGI "Jefe de Sede o de Sucursal", según Sucursal y cargo.

No.	Sucursal	Perfil exclusivo "Jefe Sede Sucursal" del SIGI a otros cargos	
		Cargo	Cantidad
1	Sucursal de Guadalupe	• ADMINIST.SUCURSAL 4 • PROFESIONAL 1 • TEC EN ADMINIS.	2 1 1
			4
2	Sucursal de Heredia	• OPERADOR EN TIC. • ADMINIST.SUCURSAL 4 • ANAL. SIST. 4 TI • INSP.LEYES REGLA.3	2 1 1 1
			5
3	Sucursal Ciudad Neily	• ADMINIST.SUCURSAL 2 • ASIST.TEC. ADMON 2 • INSP.LEYES REGLA.3	1 1 1
			3
4	Sucursal de Cartago	• ADMINIST.SUCURSAL 4 • TEC. EN ADMINIS. 5 • ANAL. SIST. 4 TIC	1 1 1

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

No.	Sucursal	Perfil exclusivo "Jefe Sede Sucursal" del SIGI a otros cargos	
		Cargo	Cantidad
			3
5	Sucursal de Turrialba	• INSP.LEYES REGLA.3 • ADMINIST.SUCURSAL 3 • ANAL. SIST. 4 TIC.	1 1 1
			3

Fuente: Elaboración propia con los datos suministrados en DAGP-0952-2019 y DAP-883-2019

2.28. El SICERE y los sistemas conexos manejan un modelo desconcentrado de asignación de roles, en el cual existen Administradores de Usuarios ubicados en la dependencia Dirección SICERE y en cada uno de los CGI (Centros de Gestión de la Información), y son los encargados de crear, eliminar y bloquear usuarios, así como asignar o eliminar los perfiles de usuario. Cada uno de estos administradores deben tener asignados todos los perfiles de cada sistema para su asignación a otros usuarios, ya que así fue diseñado el sistema. Dentro de este contexto, mediante el análisis realizado con la ejecución de la presente auditoría, se detectaron usuarios que presentan hasta 62 perfiles activos asignados.

2.29. La debilidad de gestión oportuna en los roles y perfiles para los usuarios de SICERE se puede asociar a una falta de rectoría por parte de la Dirección SICERE que garantice la comunicación entre esta Dirección y la Dirección de Administración y Gestión de Personal, así como con los CGI, para que existan los procedimientos de gestión de los perfiles debidamente aprobados y se conviertan en vinculantes para todos los actores, puestos en práctica con un control efectivo que garantice la revisión y ajustes permanentes de los accesos para minimizar el riesgo de perfiles indebidos por movimientos de personal: cambios de puestos, salidas de funcionarios u otros que modifiquen la relación laboral.

2.30. En este sentido, el "Manual Sobre la Operativa de las Labores de Administración de Usuarios y Perfiles en el Sistema Centralizado de Recaudación" establece que la Subárea de Actualizaciones Diferidas es el encargado de supervisar todas las actividades relacionadas con el control y actualización de la información de los usuarios y perfiles en todas las dependencias a nivel nacional, sobre lo cual se constató que no cuenta con procedimientos de control vinculantes y debidamente divulgados en los que se designe a los funcionarios responsables de la supervisión y control de los usuarios y sus perfiles, y establezca entre otros aspectos, la periodicidad de la revisión y actualización de roles.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.31. Existen riesgos en la confidencialidad y manejo de la información, ya que la asignación de perfiles a los usuarios no se rige bajo el principio de "menor privilegio", el cual busca que al usuario se le asignen los privilegios de uso necesarios para desarrollar las tareas que tenga encomendadas y solamente durante el tiempo necesario.

2.32. El no contar con procedimientos y controles suficientes para asegurar los niveles de accesos de los funcionarios del sistema de recaudación de la CCSS, supone un riesgo de operación que podría desencadenar en inconsistencias o alteraciones a la información, y afectar la confidencialidad e integridad de la información en los procesos de recaudación que lleva a cabo la CCSS, a nivel de datos personales de ciudadanos y patronos, información sobre facturación, planillas, alteración de montos adeudados, manipulación de negocios por cerrar por deuda o cobro judicial, entre otros.

Insuficiencia de los controles tecnológicos

2.33. Las NCISP (N-2-2009-CO-DFOE), en su capítulo V sobre sistemas de información inciso 5.3 Armonización de los sistemas de información con los objetivos establece que "la organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI.".

2.34. Además la norma 5.6 del mismo cuerpo normativo indica que "titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo. Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad.".

2.35. Bajo el mismo cuerpo normativo el inciso 5.8 Control de sistemas de información, señala que "el jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación.".

2.36. Este Órgano Contralor se encontró que el SICERE cuenta con la aplicación Oficina Virtual - Módulo Autogestión Planilla en Línea -, la cual es utilizada por un 60% de los patronos para ingresar información respecto a sus planillas mes a mes (inclusiones de trabajadores, salarios, reportes de incapacidades, permisos sin goce de salarios, entre otros).

2.37. Dentro de este contexto, se determinó que dicha aplicación virtual no cuenta con mecanismos de control suficientes en materia de aseguramiento emitida por la CCSS. Puesto que se determinaron situaciones como las siguientes: el patrono incluye ocupaciones que no corresponden a un tipo de planilla específica, se reportan salarios altos de trabajadores, en algunos casos de ¢8,000,000 y hasta ¢12,000,000, vinculados, por ejemplo, con mujeres incapacidades por maternidad, se realiza una inscripción patronal, sin valorar su condición de trabajador independiente. Además, el sistema permite el cierre de una planilla aunque tenga trabajadores activos laboralmente, entre otros casos.

2.38. Así las cosas, en cuanto a este particular, esta Contraloría General tuvo evidencia de la existencia de solicitudes que realiza la Dirección SICERE dirigidas a instancias técnicas, relacionadas con la necesidad de implementar una serie de controles y validaciones, de cara a minimizar la posibilidad de que los patronos registren información que no se ajuste a lo que

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

establece el bloque normativo, imprecisa o con errores en la planilla, como las mencionadas en el párrafo anterior.

2.39. La calidad de la información contenida en el SICERE, se ve comprometida debido a que la Gerencia Financiera no ha garantizado razonablemente que los requerimientos de validación de datos contenidos en el bloque normativo y las reglas de negocio respectivas, sean consideradas en los controles tecnológicos que deben existir al momento que los patronos ingresan la información de sus planillas en la Aplicación Autogestión Planilla en Línea de la Oficina Virtual de la CCSS.

2.40. La CCSS enfoca los cambios y mantenimiento al SICERE en gran parte a mantener la tecnología (actualización versión de base de datos, arquitectura tecnológica) dejando con menor apoyo la mejora en operatividad y automatización de actividades laborales a través de dicho sistema que aumenten la productividad de los procesos de recaudación. A pesar del conocimiento sobre las deficiencias existentes en los controles tecnológicos, las propuestas de solución vienen de mandos medios y no se logra visualizar el apoyo e involucramiento de autoridades superiores.

2.41. Por tanto la ausencia de procesos de control que permitan validar acorde a lo establecido por la normativa definida en la Administración de la CCSS en materia al ciclo de aseguramiento, genera eventuales riesgos de evasión y subdeclaración, así como eventuales incumplimientos de la normativa vinculada con esta materia.

Riesgo en el desempeño del SICERE por el crecimiento de los "Procesos Diferidos".

2.42. La Ley General de Control Interno, (LGCI) artículo 16, inciso a), indica que las instituciones del Sector Público deben contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.

2.43. Las NCISP (N-2-2009-CO-DFOE), señalan en el inciso 5.6, que "el jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.".

2.44. La norma 1.2 del MNTGCTI, nro. R-CO-26-2007 del 7 de junio de 2007 indica que "la organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.".

2.45. Las buenas prácticas de Gobierno de las Tecnologías de Información, incluidas en COBIT 5, indican en su proceso DSS01.01 "Ejecutar procedimientos operativos" que se debe "mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.".

2.46. La CCSS indica la existencia de "programas de procesamiento masivo de información que se planifican y ejecutan diariamente en la le [sic] base de datos de SICERE", los cuales se conocen como "procesos diferidos.".

2.47. Este procesamiento en lotes surge de las solicitudes que realizan los usuarios a través de requerimientos o por recomendación técnica para dar respuesta a una necesidad específica.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Se agrupan en cinco tipos; interfaz de entrada, interfaz de salida, proceso diferido, reportes de diferidos y reportes de cobro.

2.48. Así las cosas, este Órgano Contralor tuvo evidencia de que producto de una consultoría externa la CCSS recibe el informe denominado "CCSS_E2 Análisis de procesos operativos deseado v.3.0", del 08 de julio 2016, dentro del cual en su apartado 7.2.3 se refiere específicamente a los "Procesos diferidos", en cuyo caso se indica que aunque la mayoría de dichos procesos se ejecutan fuera de horario normal de atención puede resultar que genere restricciones artificiales o de superposición de procesos, que afecten el nivel de servicio que se ofrece a los procesos internos o a los usuarios (patronos, asegurados, ciudadanos).

2.49. Además, como parte del citado informe, se encuentra el "Anexo 06-Análisis de procesos diferidos SICERE", donde se identifican un total de 175 procesos diferidos, validados a esa fecha para determinar si pueden ser sujetos de mejora. En cuyo caso, se resalta el riesgo operativo del SICERE por la existencia de esta gran cantidad de procesamientos diferidos.

2.50. A mayor abundamiento, a setiembre 2019 la Dirección SICERE reportó a esta Contraloría General un total de 234 procesos diferidos activos; se identifican 17 procesos erradicados del Anexo 6[7], debido a mejoras desarrolladas al SICERE en la validación de datos de entrada ("Actualiza teléfonos de patronos", "Actualiza teléfonos de representantes", "Validación pre-notificaciones autorización débito automático"), así como procesos para corrección de datos ("Ajuste de personas erróneas", "Proceso que corrige los seguros traslapados", "Proceso que corrige los traslapes de salarios", "Proceso que corrige más de un salario abierto para trabajadores"), entre otros.

2.51. Por lo que se puede indicar que existen 76 nuevos procesos diferidos, desglosados en 44 "Reporte_Cobros", 13 "Reportes_Diferidos", 10 "Proceso_Diferido", 7 "Interfaz_Salida" y 2 de "Interfaz_Entrada.".

2.52. Lo anterior representa un incremento del 43% de procesos diferidos en relación a julio 2016 y el mayor crecimiento se ha dado a nivel de reportes en la Dirección de Cobros, situación que atrae la atención de esta auditoría dado que es una de las direcciones considerada dentro de la encuesta aplicada, que no hace uso de soluciones de inteligencia de negocio para la toma de decisiones.

2.53. Las unidades administrativas que mayor cantidad de procesos diferidos requieren son: Dirección SICERE con 42% (98), Dirección de Cobros con 28% (67) y la Dirección Financiero Contable con 17% (39). Entre las tres abarcan un 87% de los procesos diferidos activos en el SICERE. Según se observa en el gráfico siguiente:

[7] Entregable 2: Análisis de procesos operativos deseados v.3.0, del Plan de Innovación, emitido por firma consultora.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Gráfico nro. 1

Fuente: Información obtenida del oficio DSCR-0619-2019.

2.54. El aumento de los procesos diferidos que deben ser ejecutados fuera de línea en el SICERE, se debe a la falta de planificación de crecimiento y de análisis sobre los requerimientos para que el sistema pueda generar su reportería a través de las herramientas adquiridas por la CCSS para inteligencia de negocios y Big Data, así como mejorar la actualización en línea para evitar reproceso y minimizar la carga del sistema por procesamientos masivos de información, reduciendo los riesgos de pérdida y desactualización de datos.

2.55. Por lo tanto la ejecución incorrecta de un proceso diferido puede afectar trámites o procesos asociados a los datos, cálculos o reportes que generan dichos procesos, y por ende generar que los plazos de atención aumenten, así como la complejidad de las gestiones.

2.56. Tener una cadena de procesos diferidos en crecimiento y que se ejecutan en ventanas horarias no hábiles ocasiona que la CCSS no cuente con información actualizada y oportuna para la atención de los requerimientos del asegurado, teniendo que esperar hasta que sea ejecutado el proceso diferido.

2.57. El crecimiento acelerado de los reportes de cobros en los últimos cuatro años debilita la capacidad de contar con información ágil, actualizada y oportuna para la toma de decisiones. Así como no aprovechar la suite de tecnologías en soluciones BI, Big Data, analítica predictiva que dispone la DTIC de la CCSS.

2.58. Asimismo, el crecimiento de procesos diferidos puede llegar al punto en que la franja horaria para ejecución de procesos masivos no sea suficiente y no se pueda contar con el sistema en línea debido a que no esté actualizado al momento de inicio de labores normales de la CCSS.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Ausencia de formalización del funcionamiento del Consejo Tecnológico y de la Unidad Operativa para la implementación de la Agenda Digital Institucional.

2.59. Tal como lo establece la LGCI 8292, en el artículo 7 y 12 inciso d, sobre la "obligatoriedad de disponer de un sistema de control interno y los deberes del jerarca y de los titulares subordinados.".

2.60. Así como el artículo 16 inciso b), de la misma ley, indica que las instituciones del Sector Público deben armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficientes de los recursos públicos.

2.61. También las NCISP (N-2-2009-CO-DFOE)8, inciso 5.3, que "la organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI. La adecuación de tales sistemas a los objetivos institucionales involucra, entre otros, su desarrollo de conformidad con el plan estratégico institucional, y con el marco estratégico de las tecnologías de información.".

2.62. Por su parte, estas mismas Normas, en el inciso 3.3 Vinculación con la Planificación Institucional, establecen que "La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y en consecuencia, de los riesgos correspondientes. / Asimismo, los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados estén en capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos.".

2.63. Además, la norma 1.1 del MNTGCTI, nro. R-CO-26-2007 del 7 de junio de 2007 indica que "el jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.".

2.64. Este mismo cuerpo normativo, en la norma 1.6 dispone que "el jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.".

2.65. La norma 2.1 de este mismo cuerpo normativo dispone que "La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que

[8] Emitidas por la Contraloría General de la República mediante Resoluciones N° R-CO-64-2005, N° R-CO-26-2007, N° R-CO-10-2007 del 06 de febrero del 2009.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.”.

2.66. Del mismo modo, dicha norma 5.1 de este mismo cuerpo normativo dispone que “la organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.”.

2.67. En cuanto a las buenas prácticas internacionales en Tecnologías de Información del COBIT 5, en su Principio 1 indica que se deben satisfacer las metas de las partes interesadas, mediante una estrategia corporativa factible que apoye la alineación entre las necesidades de la empresa y las soluciones y servicios de TI. La cual contiene en el proceso APO01 donde se establece que se debe gestionar mediante “...mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores”. Además señala en la práctica de gestión APO01.01 que se debe “Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.”.

2.68. Seguido, el proceso APO02 “Gestionar la Estrategia” de COBIT 5, indica que se deben “alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.”.

2.69. También la APO05 establece la gestión del portafolio de proyectos mediante “...la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.”.

2.70. La Junta Directiva de la CCSS como parte del avance en el Proyecto de Gobernanza y Gestión de las TIC, en enero del 2018, acordó la habilitación de un Consejo Tecnológico con el objetivo de asumir la toma de decisiones sobre asuntos estratégicos asociados con las TIC que inciden en la prestación de los servicios a los usuarios.

2.71. Al respecto, este cuerpo colegiado ha sesionado en cinco ocasiones, abordando temas y generando acuerdos mayoritariamente sobre el avance del Proyecto de Gobernanza y Gestión de las TIC en la CCSS, seguridad de la Información y la implementación del Enterprise Resource Planning (ERP).

2.72. Dentro de este contexto, esta Contraloría General, determinó la ausencia de políticas, lineamientos u otros marcos normativos formalmente aprobados y divulgados por el Máximo Jerarca Institucional, en torno al funcionamiento de este Consejo, es decir, estableciendo de forma concreta su ámbito de acción, potestades, responsabilidades, enfoque de trabajo, así

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

como la validación de aspectos referentes al seguimiento y cumplimiento de los acuerdos definidos en el seno de este grupo y las líneas de acción establecidas para llevar a cabo la operativa de dichos acuerdos.

2.73. Por su parte, además se encontró que, la CCSS promovió la Licitación Abreviada (2016-LA-000003-1150) por concepto de "Servicios de consultoría para el diseño del Modelo de Gobernanza de las TIC y horas de servicio por demanda para el desarrollo del Plan de Implementación Inmediata", la cual presenta dentro de los entregables elementos relacionados con los lineamientos tales como: “Marco funcional del Consejo Tecnológico”, “Modelo de toma de decisiones”, “Procesos del Consejo Tecnológico”, “Perfil funcional del consejo tecnológico.”.

2.74. Así las cosas, se evidenció que la Dirección de Tecnologías de Información y Comunicaciones (DTIC) en la sesión del 23 setiembre 2019 (002-2019) trasladó al Consejo Tecnológico para su valoración estos productos, sin embargo, estos insumos a la fecha no han sido formalmente presentados, analizados, aprobados e implementados por la Administración como un marco de gestión oficial para ese cuerpo colegiado.

2.75. Por otra parte, bajo la consigna de alinear las TIC a la estrategia institucional la Junta Directiva en la sesión No. 8818 en el artículo 22 celebrada el 17 diciembre de 2015 indica “Conformación de una agenda digital estratégica en salud (ADES) que integre en el nivel institucional las principales iniciativas, programas y proyectos en materia de TIC, que se tienen previstos para ejecutarse en el próximo quinquenio; además del fortalecimiento de la infraestructura digital, el acceso universal y la inclusión social.”, la cual es parte del Eje de Desarrollo, incluida en el tema 7: Tecnologías de Información y Comunicación con el objetivo: “Disponer de tecnologías de información y comunicación eficaces, eficientes y de calidad, que respondan a las necesidades de continuidad, cercanía y eficiencia requeridas en los servicios brindados a los usuarios internos y externos.”.

2.76. Así las cosas, conforme a lo acordado es que nace la Agenda Digital Institucional (AGEDI), agenda que fue abordada por el Consejo Tecnológico de la CCSS en la sesión, el 23 setiembre del 2019, sesión donde acordó: “Dar por aprobada la AGEDI, a través de la cual se consolidan los proyectos estratégicos aprobados con componente tecnológico que se desarrollen a nivel institucional; esto a efectos de lograr una gestión integral y eficiente de este tipo de proyectos. Cada Proyecto debe seguir una línea de aprobación según la naturaleza y el marco normativo Institucional.”.

2.77. Así las cosas, la CCSS visualiza la AGEDI como un portafolio institucional que se gestiona integrando información propia de cada proyecto y con el fin de apoyar la toma de decisiones del Consejo Tecnológico.

2.78. Dentro de este contexto, esta Contraloría General determinó que, no existe claridad sobre cuál es la unidad operativa o instancia formalmente definida, responsable de gestionar de forma integral esta agenda, en términos de seguimiento y cumplimiento de las metas, control de avances, administración del riesgo, presupuesto, control de los recursos, entre otros aspectos.

2.79. A su vez, este Órgano Contralor determinó que de los 50 proyectos incorporados en la AGEDI si bien es cierto se señala a cuáles objetivos estratégicos se encuentran alineados del Plan Estratégico Institucional (PEI) 2019-2022, no se indica en forma concreta a cuál o a cuáles de las 47 líneas de acción estratégica, del objetivo, se enfocan. Además, se carece de un detalle sobre su interrelación con cada Plan Táctico Gerencial (PTG) y Plan Presupuesto (PP).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.80. Por su parte, las autoridades de la CCSS no le han dado la prioridad requerida a las acciones para concretar la formalización del Consejo Tecnológico y de la designación de una Unidad Operativa que gestione los proyectos de la AGEDI.

2.81. La ausencia de lineamientos formalmente establecidos sobre el funcionamiento del Consejo Tecnológico, podría debilitar las capacidades de gobernanza que la CCSS pretende ejercer para una adecuada gestión de las tecnologías de información y comunicaciones, la cual debe partir de una definición concreta de responsabilidades y prácticas ejercidas por los Jerarcas y altas Gerencias con el fin de proporcionar una dirección estratégica sobre las TIC, con el fin de asegurar el valor de las inversiones y su alineamiento con los objetivos institucionales, lo anterior mediante una adecuada gestión de riesgos y uso eficiente de los fondos públicos.

2.82. La falta de un responsable de la gestión de la AGEDI, impide alinear los proyectos de componente TIC con los objetivos definidos en el PEI 2019-2022, así como generar el respectivo seguimiento en el nivel táctico y operativo, aumentando el riesgo que las inversiones en TIC no contribuyan en línea con la visión estratégica y los beneficios esperados por la Institución.

2.83. Además, la falta de definición de un responsable que se encargue de la gestión de la AGEDI de forma integral, provoca también, la desvinculación de ésta con los Planes Tácticos Gerenciales y los Planes Presupuesto.

Falta definición de la estructura organizativa de la DTIC

2.84. Las NCISP, inciso 4.5.2 Gestión de proyectos establece "que el jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda.".

2.85. Por su parte, la norma 1.5 del MNTGCTI, nro. R-CO-26-2007 del 7 de junio de 2007 indica que "La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.".

2.86. Además, la norma 2.4 "Independencia y recurso humano de la Función de TI" (MNTGCTI) determina que "… debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.".

2.87. También la Norma 2.5 de este mismo cuerpo normativo, dispone que "La organización 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.".

2.88. Asimismo, el acuerdo tercero de Junta Directiva emitido en artículo 3 de la sesión 9017, celebrada el 18 de febrero de 2019, indica: "Analizar la propuesta de Modelo Meta de organización de TIC, el cual forma parte del Modelo Meta de Gobernanza y Gestión de las TIC, y presenten en un plazo de dos meses un informe a la Junta Directiva sobre la propuesta final a considerar.".

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.89. Por último, las buenas prácticas internacionales contenidas en el proceso APO01, denominada "Gestionar el marco de gobierno de las TIC" del COBIT 5, señala en la práctica de gestión APO01.05 que se debe "Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI.".

2.90. El proceso APO07 "Gestionar los Recursos Humanos" del COBIT 5, señala en dicho proceso que se debe "Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos".

2.91. La DTIC se encuentra gestando el proyecto denominado "Proyecto Modelo de Gobernanza y Gestión de las TIC en la CCSS", este nace de la licitación abreviada No.2016LA-000003-1150 "Servicios de consultoría para el diseño del Modelo de Gobernanza de las TIC y horas de servicio por demanda para el desarrollo del Plan de Implementación Inmediata" a través de una firma consultora.

2.92. Por medio de este proyecto la CCSS busca implementar un Modelo de Gobernanza y Gestión de TIC y un Modelo de Gobernanza de la Seguridad de la Información, con base en los marcos COBIT e ITIL, y en línea con las normativas que le rige; el cual a octubre 2019 presenta una inversión de ¢765,0 millones y se estima puede llegar a un costo total de ¢1.944,4 millones.

2.93. Por su parte, la CCSS además del proyecto supra mencionado, también se encuentra gestando el proyecto denominado "Proyecto de Consultoría para la Transición a la Nueva Estructura del Nivel Central con la Administración de la Cultura Organizacional", con el apoyo de otra firma consultora.

2.94. Dicha firma dentro de sus actividades presenta un informe denominado "Estructura Organizacional Tecnologías de Información y Comunicación" el cual es una propuesta que también establece su enfoque del cómo debe ser conformada dicha estructura organizacional.

2.95. Dentro de este contexto, este Órgano Contralor tuvo evidencia que en estos momentos la CCSS tiene vigente los citados proyectos, los cuales si bien es cierto, en principio son de distinta naturaleza, actualmente están convergiendo en la definición de la estructura organizativa de las TIC en la CCSS. En cuyo caso, se determinó que dichos proyectos presentan propuestas diferentes para dicha estructura organizativa, lo cual refleja una discrepancia de criterios entre las propuestas meta de ambos proyectos.

2.96. Los dos proyectos sobre la estructura organizativa de la DTIC son patrocinados por la Junta Directiva de la CCSS en tiempos distintos, los dos tienen dentro de su alcance realizar una propuesta de la estructura de gobernanza de las TICs, y a la fecha no se ha priorizado esta definición.

2.97. Al tener que aplicar ajustes en la estructura sobre dos proyectos con enfoques distintos genera costos de reingeniería y costos económicos adicionales para la institución.

La CCSS presenta rezago en el uso de la infraestructura tecnológica y datos del SICERE para la toma de decisiones

2.98. Esta situación contraviene lo estipulado en las NCISP (N-2-2009-CO-DFOE), inciso 5.6.2 Oportunidad, el cual establece que "las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales.".

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.99. También, la norma 5.9 del mismo cuerpo normativo indica que “el jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance.”.

2.100. Además, la norma 2.3 del MNTGCTI, nro. R-CO-26-2007 del 7 de junio de 2007 establece que “la organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI.

2.101. Por otra parte, las buenas prácticas internacionales establecidas en el marco de trabajo COBIT 5, en su práctica de gestión APO09.02 indican que se debe “definir y mantener uno o más catálogos de servicios para grupos de clientes objetivo relevantes. Publicar y mantener los servicios TI activos en los catálogos.”.

2.102. Asimismo, en su proceso BAI08 implica que se debe “proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.”.

2.103. Siguiendo con la práctica de gestión BAI08.01, este proceso implica “difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).”.

2.104. El SICERE contiene información histórica y actual, la cual es altamente valiosa para la toma de decisiones financiera y operativa de la CCSS, los registros contenidos en sus bases de datos pueden generar una trayectoria y proyecciones de facturación, de recaudación, de gestión cobratoria, morosidad, así como comportamientos por tipo de seguro (Obrero-Patronal, Trabajador Independiente, seguro voluntario y por el estado, etc.).

2.105. La CCSS ha realizado esfuerzos importantes en la adquisición de servicios profesionales así como licenciamiento para la conformación de herramientas e infraestructura que le permite manejar una suite de tecnologías en la implementación de soluciones BI, Big Data, analítica predictiva.

2.106. No obstante lo anterior, se logra evidenciar mediante una encuesta aplicada a jefaturas, directores y personal operativo de unidades adscritas a la Gerencia Financiera relacionados con el SICERE y sistemas conexos, utilizados en el proceso de recaudación, que el uso de estas herramientas para el análisis de datos estratégico del SICERE ha sido muy escaso a la fecha, ya que un 60.7% requiere información para la toma de decisiones que no puede extraer directamente de los sistemas y requiere la intervención de un tercero.

2.107. Además, de dicha encuesta se desprende que el 85.2% de las jefaturas, directores indica no usar alguna solución de inteligencia de negocios para la toma de decisiones.

2.108. Existiendo ausencia de políticas, así como una estrategia que promueva el uso, disponibilidad de la infraestructura y la suite de herramientas tecnológicas para la implementación de soluciones BI, Big Data, analítica predictiva, que ayuden en la toma de decisiones sobre el aprovechamiento de los registros consignados en la base de datos del SICERE y sus conexos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.109. La situación descrita conlleva a que se tiene un gran volumen de información a la que no se le está sacando todo el provecho requerido por la institución.

2.110. Se genera mayor recargo y desgaste en el personal técnico de TIC por la dependencia que existe de los usuarios de SICERE y sistemas conexos al no contar con información de manera oportuna y eficiente por las áreas involucradas en el proceso de recaudación para la toma de decisiones.

2.111. Asimismo, la institución ha realizado grandes esfuerzos mediante la contratación de servicios profesionales aunado a la adquisición de licenciamiento y herramientas para desarrollar soluciones de inteligencia de negocios y analítica avanzada, las cuales son de un alto costo económico, y no están siendo aprovechadas de manera óptima. Aspecto de especial relevancia en el caso del SICERE, donde se cuenta con datos acumulados de más de 17 años.

3. Conclusiones

3.1. La CCSS en diciembre del 2014 aprueba el denominado "Plan de Innovación para la mejora de la gestión financiera-administrativa de la CCSS basado en soluciones tecnológicas", donde uno de sus principales componentes es el Proyecto de Modernización del SICERE, al cual se le conoce en dicha institución como “Ciclo de Aseguramiento.”.

3.2. El Ciclo de Aseguramiento lo componen un grupo de procesos que se encargan de ser el enlace entre los contribuyentes y la CCSS, por medio del cual se recauda el dinero necesario para la manutención de dos grandes áreas, como son el régimen de salud, enfermedad y maternidad, y el sistema de pensiones universal; estos grupos de procesos son: Atención al usuario, Inspección, Facturación, Cobros, Distribución y Procesos Diferidos.

3.3. Dentro del contexto, el SICERE se constituye en una herramienta tecnológica de vital importancia para la CCSS, en cuyo caso estudios realizados demuestran que el SICERE contribuye en un 67% sobre los procesos del Ciclo de Aseguramiento, pero no se ha logrado una automatización completa de las operaciones, específicamente en procesos de Control de la Cuenta Individual y Gestión para la atención de casos y procesos de cobros, entre otros.

3.4. Bajo este orden de ideas, con el desarrollo de la presente auditoría, esta Contraloría General en cuanto a la seguridad de la información del SICERE, encontró debilidades en aspectos tales como: riesgo en la continuidad de los servicios relacionados con la recaudación en la CCSS, debilidades en la gestión de permisos a usuarios para el acceso al SICERE y sistemas conexos, falta de suficiencia de los controles tecnológicos, así como, riesgo en el desempeño del SICERE por el crecimiento de los “procesos diferidos.”.

3.5. A su vez, en cuanto a la gestión y gobierno de Tecnologías de Información, se evidenció, ausencia de formalización del funcionamiento del Consejo Tecnológico y de la Unidad Operativa para la implementación de la agenda digital institucional, falta de definición de

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

la estructura organizativa de la DTIC, y rezagos en el uso de la infraestructura tecnológica y datos del SICERE para la toma de decisiones.

3.6. Dentro de este contexto, dadas las debilidades apuntadas, es criterio de este Órgano Contralor que en el tanto las autoridades de la CCSS tomen acciones para subsanarlas ello incidirá positivamente en el mejoramiento y robustecimiento del SICERE, sistema de especial relevancia dentro de la dinámica operativa de la CCSS.

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, Nro. 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución Nro. R-DC-144-2015, publicados en La Gaceta Nro. 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016.

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

A ROMÁN MACAYA HAYES EN SU CALIDAD DE PRESIDENTE EJECUTIVO O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar, aprobar e implementar un plan de continuidad servicios para el SICERE, que incluya aspectos tales como el respaldo informático, atención de incidentes y recuperación de desastres, procedimientos que deben permanecer bajo constante actualización para garantizar su apoyo efectivo a la operación del SICERE y sus sistemas conexos. Para el cumplimiento de la presente disposición, se deberá remitir a esta Contraloría General, a más tardar el 31 de agosto de 2020, una certificación de que dicho plan de continuidad fue debidamente elaborado y aprobado por la CCSS. Asimismo, a más tardar el 26 de febrero de 2021, otra certificación de que se han implementado los procedimientos de contingencia informática, atención de incidentes y recuperación de desastres del SICERE. (Ver párrafos del 2.1 al 2.16).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

A LOS MIEMBROS DEL CONSEJO TECNOLÓGICO DE LA CCSS O QUIENES EN SU LUGAR OCUPE EL CARGO

4.5. Someter a valoración y aprobación de la Junta Directiva de la CCSS, el modelo de toma de decisiones, los procesos del Consejo, reglamento y lineamientos referentes al funcionamiento del Consejo Tecnológico, que permitan establecer en forma concreta sus roles, responsabilidades, competencias, alcance y otros aspectos asociados con el direccionamiento estratégico de TIC en la Institución. Para acreditar el cumplimiento de la presente disposición, se debe remitir a más tardar, el 29 de mayo de 2020, una certificación que haga constar que el modelo de toma de decisiones, los procesos del Consejo, reglamento y lineamientos referentes al funcionamiento del Consejo Tecnológico, fueron debidamente sometidos a valoración y aprobación del Máximo Jerarca Institucional. (Ver párrafos del 2.59 al 2.83).

4.6. Someter a valoración y aprobación de la Junta Directiva de la CCSS la propuesta de la unidad o instancia responsable de gestionar en forma integral la Agenda Digital y sus funciones, considerando al menos respecto a la Agenda: seguimiento y actualización, gestión de riesgos, control presupuestario, costos directos e indirectos, nivel de avance de las proyectos. Para acreditar el cumplimiento de la presente disposición, se debe remitir a más tardar, el 29 de mayo de 2020, una certificación que haga constar que la citada propuesta fue sometida a valoración y aprobación de la Junta Directiva de la CCSS. (Ver párrafos del 2.59 al 2.83).

A ROBERTO MANUEL CERVANTES BARRANTES EN SU CALIDAD DE GERENTE GENERAL O QUIEN EN SU LUGAR OCUPE EL CARGO

4.7. Presentar ante la Junta Directiva de la CCSS una única propuesta de reestructuración de las TICs a partir de los proyectos activos (“Proyecto Modelo de Gobernanza y Gestión TIC en CCSS” y “Proyecto Reestructuración Organizacional Nivel Central de la CCSS”). Para acreditar el cumplimiento de la presente disposición, se debe remitir a esta Contraloría General a más tardar, el 29 de mayo de 2020, una certificación que haga constar que la citada propuesta de reestructuración fue debidamente presentada a la Junta Directiva de la CCSS para su debida valoración. (Ver párrafos del 2.84 al 2.97).

A LUIS DIEGO CALDERÓN VILLALOBOS EN SU CALIDAD DE GERENTE FINANCIERO A.I. O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.8. Definir e implementar acciones específicas que permitan llevar a cabo una revisión completa de todos los roles y perfiles actuales con el propósito de corregir las debilidades sobre estos accesos de los funcionarios al SICERE y sistemas conexos. Para el cumplimiento de esta disposición, se deberá remitir a la Contraloría General, a más tardar el 31 de marzo 2020, una certificación que acredite que las dichas acciones fueron definidas; así como una certificación a más tardar el 30 de setiembre de 2020 que acredite que las citadas acciones fueron debidamente implementadas. (Ver párrafos del 2.17 al 2.32).

4.9. Elaborar, divulgar e implementar mecanismos de control que permitan asegurar, de forma permanente, los niveles de acceso de los funcionarios a los sistemas de información, con la debida rectoría por parte de la Dirección SICERE, para una efectiva coordinación y revisión permanente de los accesos otorgados en los CGI, de forma que se considere al

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

menos lo siguiente: actualización de los roles y perfiles, periodicidad de revisión, y responsables de velar por el cumplimiento de dicho mecanismo. Para el cumplimiento de la presente disposición, se deberá remitir a la Contraloría General, a más tardar el 30 de junio del 2020, una certificación que acredite que dichos mecanismos fueron elaborados y divulgados. Asimismo, remitir otra certificación a más tardar el 30 de octubre de 2020, que haga constar que fueron debidamente implementados. (Ver párrafos del 2.17 al 2.32).

4.10. Elaborar e implementar mecanismos de control tecnológicos para monitorear la información que los patronos declaran en la planilla, a efectos de minimizar los potenciales riesgos que conlleva que se genere una declaración imprecisa de información por parte de los empleadores a través de los medios de presentación de la planilla con que cuenta la CCSS. Para acreditar el cumplimiento de la presente disposición, se deberá remitir a esta Contraloría General una certificación, a más tardar el 29 de mayo de 2020, de que dichos mecanismos fueron debidamente elaborados, y otra certificación a más tardar el 30 de noviembre de 2020, de que dichos mecanismos fueron debidamente implementados. (Ver párrafos del 2.33 al 2.41).

A LUIS DIEGO CALDERÓN VILLALOBOS EN SU CALIDAD DE GERENTE FINANCIERO A.I. O A QUIEN EN SU LUGAR OCUPE EL CARGO Y A ROBERT PICADO MORA EN SU CALIDAD DE DIRECTOR DE TIC A.I. O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.11. Elaborar un estudio que permita identificar cada uno de los “procesos diferidos” que pueden ser reestructurados y convertidos a procesos en línea, con el propósito de contar con información actualizada y minimizar los riesgos del procesamiento fuera de línea anotados, estudio dentro del cual además deberán definirse acciones a ser implementadas. Para acreditar el cumplimiento de la presente disposición, se deberá remitir a esta Contraloría General a más tardar el 30 de setiembre de 2020, una certificación que haga constar que dicho estudio fue debidamente elaborado y fueron definidas las citadas acciones. Asimismo, a más tardar el 31 de marzo de 2021, remitir una certificación de que se ha definido una planificación detallada con cronogramas de cumplimiento sobre cada una de las acciones a ser desarrolladas y que se ha iniciado su implementación. (Ver párrafos del 2.42 al 2.58).

4.12. Definir e implementar acciones específicas que garanticen el uso de la infraestructura tecnológica y el aprovechamiento de las soluciones de BI, Big Data, analítica predictiva, acciones que deberán contemplar al menos: como insumo el estudio de procesos diferidos de la disposición anterior y la definición de mecanismos para agilizar el análisis y aprovechamiento de los datos para la toma de decisiones. Para acreditar el cumplimiento de la presente disposición, se deberá remitir a esta Contraloría General a más tardar, al 31 de julio de 2020, un informe de avance sobre la definición de las acciones específicas indicadas. Asimismo, a más tardar al 18 de diciembre de 2020, otra certificación que haga constar que dichas acciones fueron definidas y que se ha iniciado su implementación. (Ver párrafos del 2.98 al 2.111).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

MANUEL JESUS CORRALES UMAÑA (FIRMA)

Lic. Manuel Corrales Umaña, MBA
Gerente de Área

DAMARIS VEGA MONGE (FIRMA)

Licda. Damaris Vega Monge**,** MSc
Asistente Técnico

JOSE ESPINOZA REYES (FIRMA)

Lic. José Manuel Espinoza Reyes
Coordinador

MARIO ANDRES ZAMORA MADRIZ (FIRMA)

Msc. Mario Andrés Zamora Madriz
Colaborador

ELIECER FELIPE CHAVARRIA ROJAS (FIRMA)

Eliecer Felipe Chavarria Rojas
Colaborador

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica