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

Al contestar refiérase a: **ID-102335**

AD-ATIC-0122-2023
7 de noviembre de 2023

Ingeniero
Esteban Zúñiga Chacón, jefe
Centro de Gestión Informática
GERENCIA MÉDICA – 2901

Ingeniero
Alexánder Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA – 1103

Ingeniera
Guiselle Tenorio Chacón, jefe
Centro de Gestión Informática
GERENCIA ADMINISTRATIVA – 1104

Ingeniero
Roy Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA LOGÍSTICA – 1106

Ingeniero
Giovanny Campos Alvarado, jefe
Centro de Gestión Informática
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS – 1107

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

Máster
Robert Picado Mora, subgerente
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Estimados (as) señores (as):

ASUNTO: **Oficio de Advertencia sobre los mecanismos de control que apoyan el registro de aplicaciones de software y su correspondiente modelo de datos.**

Esta Auditoría, de conformidad con el Plan Anual Operativo, así como las competencias y potestades concedidas en la Ley General de Control Interno y en atención a sus funciones preventivas, procede a emitir el correspondiente oficio de advertencia en relación con el tema indicado en el epígrafe.

1- GENERALIDADES

El software ha evolucionado para convertirse en un componente esencial en cualquier organización, desempeñando un papel fundamental en la automatización de procesos, la gestión de datos y la optimización de tareas. En los últimos años, su importancia y cantidad han experimentado un crecimiento significativo, ya que las empresas dependen cada vez más de una amplia variedad de aplicaciones y soluciones de software para llevar a cabo sus operaciones.

Este incremento resalta que para una gestión efectiva de estos recursos digitales se debe considerar la implementación de un mecanismo de control con la capacidad de desplegar información de los activos de software adquiridos o desarrollados. Esta medida garantiza una mayor eficiencia operativa, la seguridad de los datos, el cumplimiento de las normativas legales y proporciona una base sólida para la toma de decisiones estratégicas. Además, facilita una asignación más eficaz de recursos y contribuye a la reducción de riesgos en un entorno de negocio cada vez más dependiente de la tecnología.

En ese sentido, la Caja Costarricense del Seguro Social (CCSS) no es la excepción, ya que ha establecido un marco normativo en materia de desarrollo de sistemas de información, en el cual define mecanismos de control para el registro de soluciones tecnológicas de software y su correspondiente modelo de datos.

Específicamente, en las "Normas Institucionales en Tecnologías de Información y Comunicaciones, Versión 2.0.0, abril 2012", en el capítulo "3. Implementación de Tecnologías de Información y Comunicaciones" referente a "Consideraciones Generales de la implementación de TIC", apartado 3.1.1, se establece lo siguiente:

> *"Todas las unidades de trabajo deben implementar y mantener las TIC requeridas, en concordancia con el Plan Táctico en Tecnologías de Información, el Modelo de Arquitectura de Información y el Modelo de Infraestructura Tecnológica. Por lo tanto, para la implementación y mantenimiento debe: (…)*
>
> - *Atender los lineamientos establecidos en la* ***Metodología de Modelo de Datos Institucional****. (…)*
> - *Mantener actualizada la información del software adquirido o desarrollado en el* ***Catálogo Institucional de Aplicaciones Informáticas –CIAI****-." **El resaltado no pertenece al original***

A ese respecto, la documentación de apoyo que integra las regulaciones a nivel interno refuerza la definición y propósito de los mecanismos supracitados, como se detalla a continuación:

- Según la *"Metodología para el Modelo de Datos Institucionales (MDI) TIC-MDI-0001, julio 2010"*, se define al **MDI** como un mecanismo de control con el registro de los sistemas de información que han obtenido validación y sello en su modelo de datos[1], o se encuentran en dicho proceso de estandarización.

[1] Conjunto de herramientas utilizadas para construir una representación lógica de los requerimientos de información para un área funcional o para toda una organización.

En este sentido, mensualmente se publica a través de la intranet institucional el "Boletín Informativo MDI", que proporciona un informe sobre el estado actual del modelo de datos y las codificaciones institucionales.

- Por otra parte, el *"Procedimiento Registro de software en el Catálogo Institucional de Aplicaciones Informáticas (CIAI) DTIC-P-0009, febrero 2010"* indica que el **CIAI** consiste en un inventario actualizado de sistemas de información adquiridos o desarrollados en la CCSS.

Además, menciona como propósito del mecanismo de control ***"verificar que no exista a nivel institucional un sistema que cubra la funcionalidad que se requiera automatizar"***.

En ese orden de ideas, en los mecanismos de control utilizados por la CCSS, se encuentra la siguiente información:

Tabla No. 1
Total de sistemas de información registrados en el CIAI y MDI

Mecanismo de control	Información registrada
Catálogo Institucional de Aplicaciones Informáticas	183 sistemas de información. 79 soluciones de inteligencia de negocios. 24 servicios de desarrollo rápido.
Modelo de Datos Institucional	Un total de 116 soluciones tecnológicas (32 modelos de datos "En Revisión", 12 "Validados" y 72 "Sellados"

Fuente: Consultas al Catálogo Institucional de Aplicaciones Informáticas (CIAI) con fecha al 21 de agosto de 2023, así como al boletín No. 233 de junio de 2023 del Modelo de Datos Institucional (MDI).

2- OBSERVACIONES

Así las cosas, esta Auditoría Interna se refiere a los mecanismos de control relacionados al registro de aplicaciones de software y su correspondiente modelo de datos a nivel institucional, con el objetivo de que esa Administración analice el estado de ambos y defina estrategias para contrarrestar la exposición al riesgo. Lo anterior, dada la importancia de estos en la prestación de servicios tecnológicos.

En ese sentido, se hace de su conocimiento las siguientes observaciones para su valoración:

2.1 Actualización de la normativa

Como se evidencia en ambas directrices normativas, han transcurrido aproximadamente 13 años desde su última actualización. Aunque su objetivo sigue siendo el mismo, se han incorporado referencias y mejoras en los controles, así como otros ajustes.

Por ejemplo, a lo largo del tiempo, se han introducido modificaciones en los accesos web para acceder a los mecanismos de control. Además, el alcance del CIAI se ha ampliado para abarcar proyectos específicos como "soluciones de inteligencia de negocio" y "servicios de desarrollo rápido".

En consecuencia, se vuelve imperativo proceder con la actualización de los documentos, con el fin de respaldar las consideraciones contenidas en el marco normativo y, al mismo tiempo, cumplir con las regulaciones que hacen referencia a dicha responsabilidad.

A ese respecto, la Ley No. 8292: Ley General de Control Interno, artículo 15. Actividades de control, indican lo siguiente:

> *"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
>
> *a) **Documentar, mantener actualizados y divulgar internamente**, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*
>
> *b) **Documentar, mantener actualizados y divulgar internamente** tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
>
> *i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.*
>
> *ii. La protección y conservación de todos los activos institucionales.*
> *iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.*
>
> *iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.*
>
> *v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación" **El resaltado no pertenece al original.***

2.2 Sobre el cumplimiento normativo en la utilización de los mecanismos de control

A través del desarrollo de diversos productos de auditoría relacionados con la utilización y gestión de sistemas de información institucionales, se ha procedido a examinar si dichos aplicativos están debidamente integrados en el MDI y CIAI. En ciertas instancias, se ha observado que los sistemas dejan de operar sin que se efectúen los ajustes necesarios o se implementan nuevas soluciones de software sin gestionarse lo correspondiente.

En consecuencia, se han solicitado actualizaciones o ajustes en los mecanismos de control de varios aplicativos. A continuación, se presentan algunos ejemplos:

Tabla No. 2
Productos de Auditoría: Revisión y Mejoras en el Registro de Información en el CIAI y MDI

Producto de Auditoría	Sistema de información evaluado
AD-AOPER-0064-2023 31 de mayo de 2023	Sistema Integrado de Planificación Novaplan.
ATIC-0042-2023 11 de julio de 2023	Software Sistema Fondo de Ahorro y Préstamo, Sistema Fondo de Retiro, Seguimiento Acuerdos Junta Administrativa FRAP, Sistema Fondo de Retiro, Ahorro y Préstamo, Sistema de Fondo de Ahorro y Préstamo CCSS, Sistema de Fondo de Retiro Empleados de la CCSS, Sistema del Fondo de Retiro, Ahorro y Préstamo (FRAP), Sistema del Fondo de Ahorro y Préstamo versión web (FRAPW), Sistema del Fondo de Ahorro y Préstamo (SFRP).
ASS-072-2021 22 de septiembre de 2021	Solución informática destinada a apoyar el control de inventario y facturación de insumos para terapia endovascular.
AD-ATIC-1596-2021 3 de agosto de 2021	Sistema de Información SI-AES.
AD-ATIC-605-2021 12 de marzo de 2021	Sistema de información que apoya el proceso de vacunación contra COVID-19

Fuente: Consultas al Catálogo Institucional de Aplicaciones Informáticas (CIAI) con fecha al 21 de agosto de 2023, así como al boletín No. 233 de junio de 2023 del Modelo de Datos Institucional (MDI).

En respuesta a estas situaciones, donde se ha encontrado esta problemática, se han emitido recomendaciones instando a los propietarios de los aplicativos a verificar la información y efectuar los ajustes necesarios.

Lo anterior, en alineamiento a las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado “XII. Administración Infraestructura Tecnológica”, señala:

> *“La institución debe implementar prácticas formales que permitan mantener identificados y* ***actualizados*** *los activos de TI, mediante* ***inventarios de recursos tecnológicos*** *instalados en la organización (hardware,* ***software****,* ***aplicaciones****, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas.”* ***El resaltado no pertenece al original.***

En ese contexto, la implementación de revisiones periódicas de esta problemática, en conjunto con la notificación por parte del nivel rector de Tecnologías de la Información y Comunicaciones a nivel institucional, dirigida a los responsables de los aplicativos y/o los enlaces gerenciales, podría contribuir de manera significativa a garantizar una actualización precisa del registro.

Es decir, esta medida reforzaría la comprensión de las responsabilidades de todas las partes implicadas en mantener actualizados los cambios que surgen, e incentivar el cumplimiento efectivo del marco normativo en relación con la atención de requisitos propios del desarrollo de software a nivel institucional.

2.3 Calidad y completitud de la información contenida en los mecanismos de control

Al examinar los datos registrados en el Catálogo Institucional de Aplicaciones Informáticas (consultado el 21 de agosto de 2023), se identificaron ejemplos (véase documento adjunto) que permiten evaluar la calidad y la completitud de la información almacenada en la sección de "Sistemas de Información", a saber:

- En 9 aplicaciones, no se proporciona el nombre del sistema de información.
- En 31 sistemas de información, falta la descripción de la funcionalidad del aplicativo.
- Solo 11 aplicativos de software incluyen la información de "nota de aprobación MDI", a pesar de que el MDI hace referencia a una cantidad superior de aplicativos que han pasado por este proceso.
- Al menos 81 registros de soluciones tecnológicas carecen del nombre del funcionario que actúa como contacto a nivel de negocio.
- En 90 registros, no se especifica el contacto por parte del personal de informática encargado del soporte.

La observación previa resalta cuestiones que podrían socavar la integridad de los mecanismos de control, contraviniendo lo dispuesto en la Ley General de Control Interno, concretamente en el artículo 8, que establece:

> *"Se entenderá por sistema de control interno, la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:*
>
> *a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal. b)* ***Exigir confiabilidad y oportunidad de la información****. c) Garantizar eficiencia y eficacia de las operaciones. d) Cumplir con el ordenamiento jurídico y técnico".* ***El resaltado no pertenece al original.***

Además, las Normas de Control Interno para el Sector Público de la Contraloría General de la República, en el numeral, 5.6 Calidad de la información, señala:

> *"5.6 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.*
>
> *Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad."*

Por consiguiente, resulta de vital importancia realizar una revisión minuciosa y comunicar lo correspondiente a las partes interesadas, asegurando razonablemente que la herramienta de inventario y control sea eficaz, cumpliendo con los objetivos para los cuales fue diseñada.

3- CONSIDERACIONES FINALES

Como se ha destacado, la importancia de los mecanismos de control en el registro de aplicaciones de software y sus modelos de datos a nivel institucional desempeñan un papel fundamental en la prestación de servicios tecnológicos y son vitales para evaluar su estado y desarrollar estrategias para mitigar riesgos.

Para tales efectos, es importante que el marco normativo vinculado a la definición de dichos mecanismos de control o propiamente los documentos internos, se revise actualice y divulgue, en alineamiento con lo definido para la generación y administración de normativa y documentación de soporte a los procesos, servicios y operaciones de TIC,

En cuanto al cumplimiento normativo, es esencial supervisar y respaldar el uso y aprovechamiento adecuado del MDI y CIAI, especialmente considerando que son componentes clave en el cumplimiento de los requisitos relacionados con el desarrollo de software a nivel institucional. Para fortalecer la responsabilidad compartida (rector TIC, Centros de Gestión Informática Gerenciales y representante del negocio), sería apropiado considerar la implementación de campañas destinadas a promover la organización de los datos existentes y a incentivar su mantenimiento.

De lo contrario, las partes involucradas podrían no utilizar adecuadamente los mecanismos de control, comprometiendo el cumplimiento de la normativa y, al mismo tiempo, reduciría el valor agregado que busca obtenerse a través de esta medida.

Finalmente, no se deben descuidar los aspectos de calidad y la completitud de la información, con el propósito de preservar la integridad de los mecanismos de control, garantizando que los datos registrados sean coherentes y precisos; aspecto esencial para respaldar la toma de decisiones a nivel institucional relacionadas con este tipo de activos TIC.

En virtud de lo expuesto, esta Auditoría previene y advierte a la Administración sobre los aspectos mencionados en el presente oficio, con el objetivo de fortalecer la comunicación con todas las partes involucradas para asegurar la eficacia y la eficiencia de los mecanismos de control, garantizando que estas herramientas cumplan su propósito y sean un componente valioso en la gestión de la Tecnologías de Información y Comunicaciones de la institución.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para administrar el riesgo y brindar la atención de la situación comunicada, en el **plazo de 1 mes** a partir del recibido de este documento

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.11.14 10:24:00 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

Anexo (1)

1. Ejemplos referentes a la calidad y completitud de la información contenida en el CIAI.

C.Auditoría-1111

Referencia: ID-102335