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

Al contestar refiérase a: **ID-133503**

AS-ATIC-0018-2025
21 de febrero de 2025

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 – 1169

Ingeniero
Roy Ovares Valerio, jefe
CENTRO DE GESTIÓN INFORMÁTICA GERENCIA DE LOGÍSTICA – 1109

Ingeniero
Giovanny Campos Alvarado, jefe
CENTRO DE GESTIÓN INFORMÁTICA GERENCIA INFRAESTRUCTURA Y TECNOLOGÍA – 1108

Ingeniero
Marco Vinicio Jiménez, jefe
CENTRO DE GESTIÓN INFORMÁTICA GERENCIA DE PENSIONES – 9108

Estimados señores (as):

ASUNTO:	**Oficio de asesoría respecto al análisis de datos registrados por el System Center Configuration Manager (SCCM) sobre la gestión centralizada de los equipos de cómputo.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2025 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, específicamente en su rol de asesor, esta Auditoría emite observaciones en torno a la gestión centralizada de los equipos de cómputo institucionales basado en el análisis de datos realizado al System Center Configuration Manager SCCM, según información aportada por la Mesa de Servicios Institucional.

Como es de su conocimiento, el System Center Configuration Manager (SCCM) es la herramienta utilizada por la institución para gestionar de manera centralizada todos los dispositivos conectados a la red. Esta plataforma desempeña un papel importante en la administración de equipos, permitiendo un

monitoreo constante y detallado de su estado, así como facilitando la implementación de actualizaciones, parches de seguridad y otras tareas esenciales de mantenimiento, la capacidad de gestionar dispositivos a gran escala, hace que el SCCM optimice el tiempo de los administradores de TI, asegurando que los sistemas se mantengan actualizados, operativos y seguros en todo momento.

La importancia de SCCM y la información que este sistema proporciona es innegable. Los datos recopilados permiten identificar de manera periódica posibles vulnerabilidades dentro de la infraestructura tecnológica, lo que facilita su corrección antes de que se conviertan en amenazas reales.

Este enfoque proactivo contribuye significativamente a la seguridad general de la red, previniendo incidentes que puedan comprometer la integridad de los sistemas y la información.

En este contexto, la Auditoría, como parte de su rol de vigilancia y control, llevará a cabo análisis continuos y regionalizados de los datos proporcionados por SCCM, a través de los productos denominados Auditoría Continua, los cuales serán fundamentales para detectar posibles riesgos y garantizar que la administración tome las acciones correctivas necesarias de forma oportuna, minimizando la posibilidad de que estos riesgos se materialicen. De esta manera, contribuir al fortalecimiento de seguridad y la continuidad operativa sin interrupciones significativas.

1. Datos del SCCM

La gestión adecuada de los equipos informáticos dentro de la institución es relevante para garantizar la seguridad, el rendimiento y la operatividad de la infraestructura tecnológica. En este sentido, la existencia de equipos registrados en el sistema System Center Configuration Manager (SCCM) no actualizados representa un riesgo.

Al 5 de febrero del 2025, se identifican 38,018 equipos a nivel institucional con el agente SCCM, los cuales se distribuyen por estado de actualización de la siguiente forma:

Tabla Nº1
Equipos con agente SCCM por estado

ESTADO	EQUIPOS
Actualizado Enero	23,133
Actualizado Diciembre	7,603
Desactualizado - Más de dos meses	6,252
Desactualizado - Requiere Upgrade S.O.	1,006
Desactualizado - No administrado, versión preview S.O.	23
Indefinido - sin registro de inventario	1
Total general	**38,018**

Fuente: Reporte SCCM a febrero 2025. Dirección de Tecnologías de Información y Comunicaciones.

Llama la atención los 7,282 equipos registrados como desactualizados, los cuales se ubican según la siguiente distribución:

Tabla Nº2
Equipos desactualizados agrupados por gerencia y/o región

UNIDAD	EQUIPOS
GERENCIA MÉDICA - HOSPITALES NACIONALES Y ESPECIALIZADAS	1,373
GERENCIA MÉDICA - REGION CENTRAL NORTE	1,104
GERENCIA MÉDICA - REGION CENTRAL SUR	1,036

UNIDAD	EQUIPOS
GERENCIA MÉDICA - REGION PACÍFICO CENTRAL	747
GERENCIA MÉDICA - REGION CHOROTEGA	700
GERENCIA MÉDICA - REGION BRUNCA	543
GERENCIA MÉDICA - REGION HUETAR ATLANTICA	456
GERENCIA MÉDICA - REGION HUETAR NORTE	308
SEDE CENTRAL GERENCIA MÉDICA	227
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS	133
NO ESPECIFICA	128
GERENCIA DE LOGISTICA	98
GERENCIA GENERAL	77
GERENCIA ADMINISTRATIVA	67
GERENCIA DE PENSIONES	66
GERENCIA MÉDICA - UNIDAD CENTROS ESPECIALIZADOS	60
GERENCIA FINANCIERA	43
PRESIDENCIA EJECUTIVA	25
GERENCIA MÉDICA	23
GERENCIA FINANCIERA - REGION CENTRAL SUCURSALES	21
UNIDADES ASESORAS DE LA PRESIDENCIA EJECUTIVA	15
GERENCIA FINANCIERA - HUETAR ATLANTICA SUCURSALES	9
GERENCIA FINANCIERA - REGION BRUNCA SUCURSALES	4
GERENCIA FINANCIERA - REGION CHOROTEGA SUCURSALES	2
GERENCIA MÉDICA - PROVEEDORES EXTERNOS	2
GERENCIA FINANCIERA - REGION HUETAR NORTE SUCURSALES	1
Total general	**7,282**

Fuente: Reporte SCCM a febrero 2025. Dirección de Tecnologías de Información y Comunicaciones.

Estos equipos representan un punto crítico de vulnerabilidad, ya que, si no se implementan actualizaciones periódicas, configuraciones adecuadas y parches de seguridad, se aumenta significativamente el riesgo de exposición a ciberataques, fallos en el sistema, pérdida de datos o interrupciones operativas.

La falta de actualizaciones sobre estos dispositivos podría permitir la proliferación de software malicioso, intrusiones no autorizadas e incluso el incumplimiento de normativas de seguridad, lo que podría derivar en consecuencias legales y reputacionales.

Por lo que esta Auditoría, considera imperativo la ejecución de las acciones necesarias para que los equipos estén configurados de manera segura, con las actualizaciones al día y cumpliendo con los estándares establecidos para mitigar cualquier posible riesgo y proteger los activos informáticos de la institución.

Por otro lado, en cuanto a los sistemas operativos, se visualiza un riesgo en el funcionamiento de equipos con versiones no actualizadas, lo cual se puede observar según la fecha de finalización de soporte tal y como se detalla en el cuadro siguiente:

Tabla Nº3
Cantidad de equipos por versión y su fecha de finalización de soporte

VERSIÓN S.O.	FIN SOPORTE	EQUIPOS
Server 2012 R2	09/10/2023	4
Server 2016	12/06/2027	415
Server 2019	09/06/2029	779
Server 2022	14/10/2031	302
W10 1507	14/10/2025	2
	Soporte finalizado antes del 2022	1

VERSIÓN S.O.	FIN SOPORTE	EQUIPOS
W10 1511	Soporte finalizado antes del 2022	2
W10 1607	13/10/2026	13
	Soporte finalizado antes del 2022	9
W10 1703	Soporte finalizado antes del 2022	17
W10 1709	Soporte finalizado antes del 2022	7
W10 1803	Soporte finalizado antes del 2022	21
W10 1809	Soporte finalizado antes del 2022	34
W10 1903	Soporte finalizado antes del 2022	23
W10 1909	Soporte finalizado antes del 2022	91
W10 2004	Soporte finalizado antes del 2022	5
W10 20H2	Soporte finalizado antes del 2022	12
W10 21H1	Soporte finalizado antes del 2022	7
W10 21H2	13/06/2023	27
	11/06/2024	25
W10 22H2	14/10/2025	6295
	Indefinido - validar de forma manual	1
W11 21H2	10/10/2023	275
	08/10/2024	270
W11 22H2	08/10/2024	177
	14/10/2025	134
W11 23H2	10/11/2026	14022
	11/11/2025	9755
W11 24H2	13/10/2026	2723
	12/10/2027	2543
	Indefinido - validar de forma manual	3

Fuente: Reporte SCCM a febrero 2025. Dirección de Tecnologías de Información y Comunicaciones.

La distribución de estos equipos por región se presenta en la siguiente tabla, con enfoque brinda la cantidad de equipos con versiones obsoletas.

Tabla Nº4
Cantidad de equipos con sistema operativo sin soporte por gerencia

UNIDAD	EQUIPOS
GERENCIA MEDICA - HOSPITALES NACIONALES Y ESPECIALIZADAS	255
GERENCIA MEDICA - REGION CENTRAL NORTE	228
GERENCIA MEDICA - REGION CENTRAL SUR	124
GERENCIA MEDICA - REGION HUETAR ATLANTICA	91
GERENCIA MEDICA - REGION CHOROTEGA	85
GERENCIA MEDICA - REGION PACIFICO CENTRAL	54
GERENCIA MEDICA - REGION HUETAR NORTE	27
GERENCIA MEDICA - REGION BRUNCA	26
GERENCIA DE PENSIONES	26
GERENCIA MEDICA - UNIDAD CENTROS ESPECIALIZADOS	24
SEDE CENTRAL GERENCIA MÉDICA	15
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS	12
GERENCIA DE LOGISTICA	9
GERENCIA ADMINISTRATIVA	8
GERENCIA GENERAL	6
GERENCIA FINANCIERA.	5
Otros dominios CAJA	4
GERENCIA FINANCIERA - REGION CENTRAL SUCURSALES	2
UNIDADES ASESORAS DE LA PRESIDENCIA EJECUTIVA	2
Total general	**1007**

Fuente: Reporte SCCM a febrero 2025. Dirección de Tecnologías de Información y Comunicaciones.

Es necesario señalar que la falta de actualizaciones periódicas de los sistemas operativos representa un riesgo significativo para la seguridad y la operatividad de los dispositivos dentro de la red institucional.

De la información suministrada se identifican equipos que operan con versiones obsoletas de Windows 10 (desde la versión 1507 hasta la 21H2) y Windows 11 (versión 21H2 a la 22H2). Estas versiones desactualizadas no solo carecen de las últimas mejoras en cuanto a rendimiento y funcionalidad, sino que además carecen de los parches de seguridad necesarios para protegerse contra vulnerabilidades conocidas.

Además, las versiones más antiguas, como Windows 10 1507, 1511 o 1607, ya no son compatibles con actualizaciones de seguridad, lo que deja a los dispositivos que funcionan con las mismas, expuestos a posibles amenazas cibernéticas como malware, ransomware y ataques de día cero.

Adicionalmente, esta situación podría generar incompatibilidades con nuevos softwares o hardware, lo que afectaría la productividad y eficiencia operativa.

2. Equipos sin el cliente SCCM

Por otro lado, se identificó 7,656 equipos dentro de la institución que no están registrados como clientes en el System Center Configuration Manager (SCCM). Esta condición presenta un riesgo considerable, ya que no pueden ser contemplados en la gestión centralizada de dispositivos realizada mediante esta herramienta y por ende no disponer de las actualizaciones de seguridad, ni configuraciones de políticas necesarias, lo que los hace vulnerables a amenazas cibernéticas y/o riesgos de continuidad.

Además, la falta de mapeo adecuado de estos dispositivos dificulta la capacidad de la organización para mantener un inventario preciso y cumplir con la normativa aplicable en materia de ciberseguridad y seguridad de la información. A continuación, se muestra la cantidad de equipos identificados en esta situación agrupados por gerencia o región:

Tabla Nº5
Cantidad de equipos sin agente SCCM por gerencia

UNIDAD	EQUIPOS
GERENCIA MEDICA - HOSPITALES NACIONALES Y ESPECIALIZADAS	1964
GERENCIA MEDICA - REGION CENTRAL NORTE	1272
GERENCIA MEDICA - REGION CENTRAL SUR	758
GERENCIA MEDICA - REGION CHOROTEGA	559
GERENCIA MEDICA - REGION PACIFICO CENTRAL	551
GERENCIA MEDICA - REGION HUETAR ATLANTICA	359
GERENCIA DE LOGISTICA	282
GERENCIA MEDICA - REGION HUETAR NORTE	272
GERENCIA GENERAL	271
GERENCIA MEDICA - REGION BRUNCA	250
Otros dominio CAJA	163
GERENCIA ADMINISTRATIVA	159
SEDE CENTRAL GERENCIA MÉDICA	159
GERENCIA DE PENSIONES	148
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS	102
GERENCIA MEDICA - UNIDAD CENTROS ESPECIALIZADOS	79
PRESIDENCIA EJECUTIVA	74
GERENCIA FINANCIERA	71
UNIDADES ASESORAS DE LA PRESIDENCIA EJECUTIVA	67

AUDITORIA	34
GERENCIA FINANCIERA - REGION CENTRAL SUCURSALES	26
GERENCIA FINANCIERA - HUETAR ATLANTICA SUCURSALES	22
GERENCIA FINANCIERA - REGION HUETAR NORTE SUCURSALES	6
GERENCIA FINANCIERA - REGION CHOROTEGA SUCURSALES	3
GERENCIA MEDICA - PROVEEDORES EXTERNOS	2
GERENCIA MÉDICA	2
GERENCIA FINANCIERA - REGION BRUNCA SUCURSALES	1
Total general	**7656**

Fuente: Reporte SCCM a febrero 2025. Dirección de Tecnologías de Información y Comunicaciones.

3. Consideraciones Normativas

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT, en el apartado XI sobre "Seguridad y Ciberseguridad", señala:

> "*La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.*
>
> *La institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, danos e interferencia a la información y los activos de información de la institución.*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*
>
> *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.*
>
> *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios".*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones indica como parte de la Gestión Estratégica del nivel Dirección, lo siguiente:

> "*Proponer al Consejo de Presidencia y Gerentes la actualización y modernización del hardware y software para la prestación efectiva de los servicios a lo usuarios, de conformidad con los requerimientos institucionales y los resultados de los procesos de investigación, a efecto de incrementar la oportunidad y la calidad de los servicios."*

"Participar en la definición y recomendación de especificaciones de tecnologías de información y comunicaciones de uso interno, de acuerdo con los requerimientos de los usuarios, con el fin de salvaguardar los intereses y facilitar la prestación de los servicios."

"Planificar, coordinar, controlar y evaluar a nivel macro la gestión de las áreas de trabajo adscritas y los resultados globales, con base en los procesos de trabajo aprobados, la programación operativa, los planes, los instrumentos de control establecidos y los informes de labores, con el propósito de satisfacer con oportunidad y calidad las demandas de los usuarios y definir las medidas correcticas en caso necesario"

El Modelo Organización de los Centros de Gestión Informática, como parte de la Gestión Técnica, de los Centros de Gestión Informática Gerenciales, refiere al respecto:

"Elaborar e implementar planes de seguridad y calidad informática, con fundamento e la normativa vigente, el aseguramiento de los recursos informáticos (hardware, software y de accesibilidad a los CGI) y de las comunicaciones, con el propósito de mantener un servicio que se caracterice por la integridad, confidencialidad y disponibilidad.

Implementar medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus, con base en la programación operativa y los antivirus disponibles, (licencias), con el fin de garantizar la confiabilidad y seguridad de la información.

Desarrollar acciones de seguridad en la implementación y el mantenimiento de software e infraestructura tecnológica, de acuerdo con los lineamientos y procedimientos establecidos, con fin de evitar fallas operativas, daños o pérdida de información".

Y como parte de sus actividades sustantivas, describe:

"Vigilar constantemente el desempeño y suficiencia de la plataforma tecnológica.
Realizar el mantenimiento del hardware, del software y de las comunicaciones".

4. Consideraciones finales

En base a la información analizada, se ha identificado que la falta de actualizaciones periódicas, la configuración inadecuada o equipos sin registro en el SCCM, representa riesgos críticos para la seguridad y continuidad de los sistemas informáticos de la institución, así como los procesos de la CCSS dependientes de la operación de ellos.

Esta situación pone a la Caja Costarricense de Seguro Social (CCSS) en una situación vulnerable ante una amplia gama de amenazas, como la infección por software malicioso, intrusiones no autorizadas y el incumplimiento de las normativas de seguridad establecidas.

Tales vulnerabilidades pueden tener consecuencias graves, que incluyen el compromiso de la integridad y confidencialidad de los datos sensibles de la institución, así como la interrupción o alteración de procesos operativos clave. En este contexto, los riesgos asociados podrían afectar no solo la seguridad de los sistemas, sino también la reputación y la capacidad operativa de la CCSS, exponiéndola eventualmente a sanciones legales y pérdidas económicas derivadas de posibles brechas de seguridad.

Por lo tanto, es importante que, en conjunto con las unidades pertinentes, se tomen las medidas inmediatas y efectivas para gestionar oportunamente estos riesgos y garantizar que todos los equipos informáticos, sistemas operativos y aplicaciones estén debidamente actualizados y configurados conforme a los estándares de ciberseguridad institucionales, así como los definidos por mejores prácticas mundiales.

Entre las acciones prioritarias se incluyen la implementación de actualizaciones periódicas de software y parches de seguridad, así como la configuración y monitoreo constante de los sistemas para detectar y prevenir posibles amenazas.

Además, se sugiere establecer un proceso de monitoreo continuo para asegurar que se mantengan los más altos niveles de protección, reduciendo significativamente el riesgo de incidentes de seguridad y asegurando el cumplimiento de las normativas y estándares nacionales e internacionales aplicables.

Atentamente,

AUDITORÍA INTERNA

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/JPS/ayms

Anexo: Listado equipos SCCM.xls

C. Auditoría.
Máster. Mónica Taylor Hernández, presidenta, Presidencia Ejecutiva - 1102
Doctor. Alexander Sánchez Cabo, gerente a.i. Gerencia Médica – 2901
Máster Gabriela Artavia Monge, gerente, a.i. Gerencia Administrativa - 1104
Licenciado. Gustavo Picado Chacón, gerente, Gerencia Financiera - 1103
Ingeniero. Jorge Granados Soto, gerente, Gerencia Infraestructura y Tecnologías - 1107
Doctor. Esteban Veja De La O, gerente, Gerencia Logística - 1106
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia Pensiones – 9108
Ingeniero. Robert Picado Mora, subgerente, Dirección De Tecnologías De Información Y Comunicaciones-1150

Referencia: ID-133503