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

Al contestar refiérase a: **ID-130437**

AS-ATIC-0001-2025
6 de enero de 2025

Ingeniera
Giorgianella Araya Araya, directora
DIRECCIÓN DE SERVICIOS INSTITUCIONALES - 1161

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

Estimado(a) señor(a):

ASUNTO: **Oficio de Asesoría referente a la gestión y/o modernización de Sistemas de Videovigilancia desde la perspectiva del apoyo que brindan las Tecnologías de la Información y Comunicación (TIC).**

En cumplimiento del programa de actividades especiales consignadas en el Plan Anual Operativo de esta Auditoría para el período 2025 y con fundamento en las competencias establecidas en los artículos 21 y 22 de la Ley General de Control Interno, se emite la presente asesoría sobre la gestión y/o modernización de Sistemas de Videovigilancia en la Caja Costarricense de Seguro Social (CCSS) desde la perspectiva del apoyo que brindan las Tecnologías de la Información y Comunicación (TIC), con la finalidad de proporcionar a la administración elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones en relación con este tema.

1. GENERALIDADES

La gestión de sistemas de videovigilancia en la CCSS durante varias décadas utilizó exclusivamente tecnologías analógicas que permitían el monitoreo de áreas específicas, esto mediante cámaras con la capacidad de capturar imágenes y almacenarlas en dispositivos dedicados (como discos compactos o discos duros), mientras que la visualización de las grabaciones se realizaba a través de monitores interconectados en un entorno físico delimitado.

En ese sentido, esa tecnología proporcionaba una solución funcional para la supervisión en tiempo real y la grabación de imágenes; sin embargo, la infraestructura presentaba limitaciones debido a necesidades específicas, especialmente en términos de flexibilidad operativa y acceso remoto.

Ahora bien, las oportunidades del mercado comenzaron a impulsar el desarrollo de nuevas soluciones tecnológicas orientadas a mejorar la cobertura, la gestión, la accesibilidad y otros aspectos clave relacionados con la capacidad de estos dispositivos, aprovechando al máximo la infraestructura de las Tecnologías de la Información y Comunicación.

Es decir, con la evolución de las TIC, los sistemas de videovigilancia, al igual que otros procesos institucionales, encontraron en este ámbito un soporte crucial que facilitó una transformación significativa en su funcionamiento y eficiencia.

En particular, la digitalización de estos procesos permitió la integración de cámaras conectadas mediante redes IP[1], lo que facilitó el acceso a las imágenes desde una amplia variedad de dispositivos, incluyendo monitores, televisores, teléfonos móviles, tabletas y computadoras; básicamente cualquier equipo con conexión a la red y/o Internet.

De manera complementaria, los métodos de almacenamiento de datos progresaron significativamente, pasando de dispositivos físicos locales a servidores con capacidades ampliadas, y más recientemente, adoptando soluciones basadas en almacenamiento en la nube.

En este contexto, el crecimiento en la CCSS puede analizarse desde diversas perspectivas, y para ilustrarlo, se toma como ejemplo la información registrada en la base de datos del Sistema Contable de Bienes Muebles (SCBM), donde es posible identificar aspectos como la cantidad de activos, la concentración de equipos y la preponderancia de ciertos componentes, entre otros factores. (Ver el insumo proporcionado en el **Anexo No. 1**, el cual podrán utilizar para obtener detalles sobre las condiciones de los activos según las necesidades específicas de cada interesado).

- La consulta de los bienes realizada al 09 de diciembre de 2024 en el SCBM revela que la Institución cuenta con 951 activos que coinciden con la descripción de cámaras de seguridad, equipos de videovigilancia, cámaras IP y otros relacionados.

- La categoría con la mayor concentración de equipos corresponde a las cámaras IP, con un total de 621 activos, lo que refleja la alineación con el proceso de modernización descrito previamente y evidencia el avance en la evolución del sistema de videovigilancia.

- La mayor concentración de bienes registrados en el inventario se concentra en el periodo correspondiente al 2020, con un total de 145 equipos, seguido por 140 componentes de videovigilancia incluidos en el SCBM durante el periodo del 2021.

- La Unidad Programática (UP) con la mayor cantidad de bienes en la categoría mencionada es la 2102 – Hospital San Juan de Dios, con 167 activos; seguida por la 2531 – Área de Salud de Santa Cruz, con un total de 104 equipos y/o componente de videovigilancia.

Es relevante señalar que lo expuesto anteriormente representa solo un punto de vista que contribuye a describir el panorama general; por lo tanto, es esencial reconocer que existen otros factores que deben ser conceptualizados de manera integral, lo cual permitirá realizar una evaluación más precisa de la condición actual del sistema de videovigilancia, el cual debido a la magnitud de la institución, puede resultar amplio y complejo.

2. CONSIDERACIONES NORMATIVAS

En relación con los temas antes indicados existe un conjunto de leyes, normas, reglamentos y demás documentos que señalan deberes, derechos, definiciones y objetivos, a saber:

[1] Las redes IP son infraestructuras que permiten la interconexión de dispositivos usando direcciones IP para transmitir datos, ya sea en Internet o en una intranet.

Las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) en el Capítulo I: Normas Generales, apartado 1.4. Responsabilidad del jerarca y los titulares subordinados sobre el SCI, inciso f, establece:

> *"Las acciones pertinentes para el fortalecimiento del SCI, en respuesta a las condiciones institucionales y del entorno".*

Además, en el Capítulo IV: Normas sobre actividades de control, apartado 4.3.3 "Regulaciones y dispositivos de seguridad", indica lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben disponer y vigilar la aplicación de las regulaciones y los dispositivos de seguridad que se estimen pertinentes según la naturaleza de los activos y la relevancia de los riesgos asociados, para garantizar su rendimiento óptimo y su protección contra pérdida, deterioro o uso irregular, así como para prevenir cualquier daño a la integridad física de los funcionarios que deban utilizarlos".*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a "V. Arquitectura Empresarial", lo siguiente:

> *"La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información."*

Esas mismas Normas técnicas para la gestión y el control de las Tecnologías de Información, menciona dentro de los procesos del marco de gestión de TI, lo correspondiente a la "XI. Seguridad y Ciberseguridad":

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

Además, haciendo referencia a "Administración Infraestructura tecnológica", en el capítulo XII de las Normas técnicas para la gestión y el control de las Tecnologías de Información, se indica:

> *"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.*

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

Finalmente, en el capítulo "XIV. Aseguramiento" de los procesos del marco de gestión de TI, indica lo siguiente:

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

3. OBSERVACIONES

Dado lo expuesto, la optimización del sistema de videovigilancia de la CCSS debe estar alineado con las necesidades institucionales y las oportunidades que brindan las soluciones de vanguardia. Esto no solo para mejorar la calidad del servicio, sino que también fortalece la capacidad de respuesta ante situaciones críticas.

En ese sentido, esta Auditoría presentan una serie de observaciones que podrán ser consideradas por la Administración para diseñar, implementar o fortalecer las estrategias relacionadas con este tema.

- La Institución debe disponer de un **marco normativo** robusto y directrices claras que regulen todas las actividades relacionadas con el mantenimiento y operación de los sistemas e incluso documentación técnica sobre la configuración de las cámaras y su relación con la red y los sistemas de TIC; alineándolas tanto con las políticas internas como con las regulaciones externas aplicables, asegurando que se cumplan los requisitos legales y las mejores prácticas.

  A ese respecto, un marco normativo bien definido no solo promueve la transparencia y la rendición de cuentas, sino que también establece la identificación y entendimiento común entre todos los actores involucrados; facilitando la cooperación y garantizando que cada parte asuma y cumpla con sus responsabilidades de manera efectiva y consistente. Además, asegura la estandarización de procesos y el cumplimiento de características o labores mínimas necesarias, lo cual es crucial para mantener un nivel de calidad y coherencia en todas las operaciones.

- En cuanto a la **gestión de sistemas de videovigilancia**, resulta fundamental mantener actividades continuas de planificación y soporte, garantizando que la selección de tecnologías y el diseño de estos sean plenamente compatibles con la infraestructura TIC existente, enfoque que no solo optimiza el desempeño, sino también fomenta la interoperabilidad.

  Además, es fundamental establecer rutinas de mantenimiento preventivo y correctivo para componentes eléctricos, cámaras, servidores, almacenamiento, software y redes, que incluyan actividades como actualizaciones, limpieza, calibración y pruebas. Igualmente, se debe implementar un monitoreo periódico del software y hardware, utilizando indicadores clave o alertas que permitan evaluar en tiempo real la calidad del servicio y detectar problemas de forma temprana, lo que contribuye a minimizar los riesgos operativos.

- Para garantizar el funcionamiento eficiente de los sistemas de videovigilancia, es esencial contar con una **infraestructura de red** adecuada que soporte las demandas específicas de transmisión de video, especialmente en el caso de cámaras IP. Estas requieren una conexión estable y de alta capacidad para evitar interrupciones o degradación de la calidad de las imágenes, lo que podría comprometer la operatividad del sistema y su capacidad para cumplir con los objetivos de monitoreo.

  Por otra parte, valorar la implementación de la segmentación de la red mediante el uso de VLAN[2] dedicadas exclusivamente para las cámaras de videovigilancia, enfoque que no solo optimiza el desempeño del sistema al evitar interferencias con otros servicios, sino que también fortalece la seguridad al aislar el tráfico de video, minimizando riesgos relacionados con accesos no autorizados o posibles vulnerabilidades en la red.

  Por último, es imprescindible realizar un monitoreo constante y una planificación adecuada del ancho de banda disponible, asegurándose de que la transmisión de video no genere congestión que pueda afectar servicios críticos de la institución.

- Los **sistemas de almacenamiento y procesamiento**, incluyendo servidores NVR (Network Video Recorder) y DVR (Digital Video Recorder), deben estar adecuadamente dimensionados para garantizar su capacidad y redundancia, esencial para manejar eficientemente la carga de trabajo y evitar interrupciones en el registro de las grabaciones, ya sea que se almacenen localmente o en la nube, alineándose con los requerimientos operativos y de seguridad de la organización.

  Asimismo, es fundamental coordinar con las áreas responsables la implementación de políticas claras, documentadas y correctamente configuradas de retención de datos, garantizando que cumplan con las normativas legales aplicables y, a su vez, se ajusten a las necesidades operativas de la institución; indispensable para optimizar el uso de los recursos de almacenamiento.

[2] VLAN (Red de Área Local Virtual) es una red lógica que segmenta el tráfico de datos dentro de una red física.

- En cuanto a la **seguridad de la información** en los sistemas de videovigilancia, es fundamental implementar medidas de ciberseguridad que protejan las cámaras y los sistemas asociados de accesos no autorizados, incluyendo el uso de credenciales seguras, la actualización regular del firmware de las cámaras para corregir vulnerabilidades y la configuración de firewalls.

  Lo anterior, bajo la premisa de detectar de manera temprana intentos de intrusión, fallos de seguridad o cualquier anomalía que pueda comprometer la información sensible, integridad y/o confidencialidad de las grabaciones.

- La **sostenibilidad del sistema a largo plazo** requiere un enfoque estratégico que integre escalabilidad, planificación presupuestaria y actualización continua de las tecnologías utilizadas.

  En este sentido, es fundamental diseñar sistemas con capacidad de crecimiento, que se adapten a las necesidades futuras de la institución. Esto no solo facilita la expansión, sino que también asegura la continuidad operativa en un entorno dinámico y en constante evolución.

  Asimismo, resulta clave analizar detalladamente los costos asociados a la infraestructura tecnológica, incluyendo las licencias de software, los servicios de mantenimiento y las actualizaciones necesarias, para garantizar una gestión eficiente de los recursos.

4. CONSIDERACIONES FINALES

Ante la evolución constante de las TIC, la administración enfrenta el desafío de analizar y eventualmente incorporar nuevas tecnologías o realizar ajustes en los sistemas de videovigilancia que impulsen mejoras en los procesos, optimicen el uso de los recursos y reduzcan costos, entre otros beneficios.

No obstante, dicho accionar implica alinear las iniciativas de modernización y renovación de dispositivos con los objetivos estratégicos, tácticos y operativos de la institución, exigiendo una planificación integral que considere tanto la implementación inicial como la sostenibilidad a largo plazo de las soluciones de videovigilancia, garantizando su capacidad para satisfacer las necesidades actuales y futuras.

En este contexto, es prioritario disponer de un marco normativo robusto y actualizado que establezca lineamientos claros para respaldar la operación, el mantenimiento y la mejora continua de los sistemas podrá guiar a los responsables e interesados en la adaptación a los cambios tecnológicos y regulatorios, promoviendo la estandarización de procesos y fortaleciendo la coherencia en las prácticas operativas.

Del mismo modo, contar con una infraestructura de red adecuada y con capacidad suficiente para satisfacer las demandas de transmisión y procesamiento de video es esencial para mantener un funcionamiento eficiente y confiable de los sistemas; dado que una red bien diseñada no solo optimiza el desempeño operativo, sino que también fortalece la seguridad al reducir vulnerabilidades y asegurar la calidad de las transmisiones.

En este orden de ideas, es primordial valorar las capacidades de los sistemas de almacenamiento y su escalabilidad, considerando tanto los requerimientos operativos, como la importancia de la seguridad de la información, en aspectos vinculados con las políticas de retención de datos, medidas de ciberseguridad, integridad y confidencialidad de la información, por mencionar algunos elementos claves para cumplir con la exigencias normativas y expectativas de los usuarios.

Por otra parte, es fundamental atender la sostenibilidad de los sistemas de videovigilancia para garantizar que sigan cumpliendo con los objetivos que motivaron su implementación, asegurando un retorno de inversión adecuado y la maximización de sus beneficios; enfoque que permite hacer un uso y aprovechamiento de los recursos y fortalecer el impacto de estas herramientas en la mejora continua de la seguridad y los servicios institucionales.

Por lo anteriormente expuesto, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a esas direcciones sobre lo descrito, para que sea sometido a valoración, revisión y sea considerado en el marco de la mejora continua, fomentando la reflexión estratégica, la optimización de los procesos existentes y el reforzamiento de las actividades de control adoptadas por la administración, que finalmente se traduzcan en un impacto real en la calidad de la prestación de los servicios que brinda la CCSS.

Finalmente, se solicita respetuosamente informar a este Órgano Fiscalizador respecto a las labores efectuadas entorno a las observaciones planteadas en el presente documento.

Atentamente,

AUDITORÍA INTERNA

RANDALL JIMENEZ SABORIO (FIRMA)
Firmado digitalmente por RANDALL JIMENEZ SABORIO (FIRMA)
Fecha: 2025.01.06 11:52:53 -06'00'

Lic. Randall Jiménez Saborío, MATI
Subauditor

RJS/RAHM/OMG/lbc

Anexo(1)

1. Archivo Excel con activos de videovigilancia, registrados en la base de datos del Sistema Contable de Bienes Muebles (SCBM)

C. Máster Gabriela Artavia Monge, gerente a.i, Gerencia Administrativa- 1104.
Gerencia General – 1100.
Auditoría-1111

Referencia:ID-130437