AGO-055-2020
10 de julio de 2020

RESUMEN EJECUTIVO

El estudio se realizó de conformidad con el Plan Anual de Trabajo 2020 del Área Gestión Operativa, en el apartado de actividades programadas, con el propósito evaluar la gestión en tecnologías de información y comunicaciones en el Área de Salud Heredia-Virilla.

Los resultados del presente informe evidencian debilidades relacionadas con la gestión administrativa en aspectos como: ausencia de definición de los procesos sustantivos que ejecuta, vigencia de los riesgos incluidos en Plan de Continuidad de la Gestión, así como la no ejecución de los ensayos programados del PCTIC, carencia de planificación operativa; además de carecer de indicadores de gestión que permitan valorar el alcance de las acciones que ejecuta el encargado de la gestión en TIC del Área de Salud.

Además, en relación con la gestión operativa se evidenciaron oportunidades de mejora en aspectos como: desarrollo e implementación de protocolos de seguridad para el aseguramiento de los activos informáticos, elaboración y desarrollo de planes de capacitación, así como en el registro de atención de incidencias de soporte técnico.

Aunado a lo anterior, se evidenció el resguardo de respaldos de bases de datos institucionales por parte de funcionarios del Área de Salud, sin que se hayan establecido procedimientos que permitan asegurar que esos datos están correctamente protegidos.

En virtud de los resultados se emiten 8 recomendaciones dirigidas a las autoridades del Área de Salud Heredia-Virilla, con la finalidad de fortalecer los procesos relacionados con gestión administrativa, gestión técnica y seguridad de los equipos.

AGO-055-2020
10 de julio de 2020

ÁREA DE GESTIÓN OPERATIVA

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN EL ÁREA DE SALUD HEREDIA-VIRILLA

ORIGEN DEL ESTUDIO

El presente estudio se realizó en atención al Plan Anual Operativo del Área Gestión Operativa para el 2020, apartado de actividades programadas.

OBJETIVO GENERAL

Evaluar la gestión en tecnologías de información y comunicaciones en el Área de Salud Heredia-Virilla.

OBJETIVOS ESPECÍFICOS

- Determinar el cumplimiento de las funciones sustantivas del Centro de Gestión Informática del Área de Salud.

- Evaluar la suficiencia y oportunidad de la gestión y planificación del Centro de Gestión Informática del Área de Salud.

- Determinar aspectos relevantes de la estructura organizacional y funcional y plataforma tecnológica del Centro de Gestión Informática del Área de Salud.

ALCANCE

El estudio comprendió la revisión y análisis de las actividades sustantivas propias del Centro de Gestión Informática del Área de Salud durante el 2019, ampliándose en aquellos casos que se consideró necesario.

La evaluación se efectuó de conformidad con lo establecido en las Normas Generales de Auditoría para el Sector Público, divulgadas a través de la Resolución R-DC-064-2014 de la Contraloría General de la República.

METODOLOGÍA

Para la realización del presente estudio se aplicaron los siguientes procedimientos metodológicos:

- Análisis de Planes Anuales 2017-2018.
- Análisis del Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones.
- Verificación de protocolos de seguridad de los equipos.
- Análisis de las condiciones de seguridad física del Centro de Gestión Informática del Área de Salud Heredia-Virilla.
- Entrevista a los siguientes funcionarios del Área de Salud Heredia-Virilla:

    - Ing. Adrián Campos Rojas, encargado de Gestión Informática.
    - Dr. Gilberto Marín Carmona, Director Médico.
    - Licda. Mayra Arce Miranda, Administradora.

MARCO NORMATIVO

- Ley General de Control Interno, 8292. Julio, 2002.
- Normas de Control Interno para el Sector Público, R-CO-9-2009 Contraloría General de la República, febrero 2009.
- Manual de Organización de Centros de Gestión Informática, Caja Costarricense del Seguro Social, octubre 2013.
- Manual para elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, Caja Costarricense de Seguro Social, mayo 2013.
- Modelo de Funcionamiento y Organización de las Áreas de Gestión de Bienes y Servicios, diciembre 2005.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría informa y previene a los jerarcas y a los titulares subordinados acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37, 38 de la Ley General de Control Interno 8292 referente al trámite de las evaluaciones efectuadas; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"Artículo 39. Causales de responsabilidad administrativa - El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)".*

ANTECEDENTES

El Área de Salud Heredia Virilla se clasifica como tipo 1 y se encuentra localizada en el cantón central de la provincia de Heredia, comprende los distritos de San Francisco y Ulloa, la sede principal se ubica al costado norte de la escuela de Guararí. Actualmente está constituida por 5 sectores, a saber: Guararí, Lagos, Lagunilla, Milpa, Aurora y Barreal, en los cuales se ubican 14 Ebáis. El centro hospitalario de referencia es el hospital San Vicente de Paúl.

Los procesos relacionados con la Gestión de Tecnologías de Información y Comunicaciones están a cargo del Ing. Adrían Campos Rojas, quien además tiene bajo su responsabilidad el registro y control de activos del Área de Salud.

HALLAZGOS

1. GESTIÓN ADMINISTRATIVA DEL ENCARGADO DE GESTIÓN INFORMÁTICA DEL ÁREA DE SALUD HEREDIA-VIRILLA

Se evidenciaron debilidades en la gestión administrativa del encargado de Gestión Informática del Área de Salud Heredia-Virilla en aspectos relacionados con la definición de los procesos sustantivos, vigencia de los riesgos incluidos en Plan de Continuidad de la Gestión, ejecución de ensayos de los procedimientos de recuperación, ausencia de planificación operativa, así como indicadores de gestión que permita medir el cumplimiento de las metas y objetivos planteados en TIC, según se detalla seguidamente:

1.1 Definición de los procesos sustantivos del encargado de Gestión Informática

Se evidenció que la administración del Área de Salud Heredia-Virilla no ha definido los procesos sustantivos de Gestión Informática, ni documentado formalmente las acciones que debe ejecutar el funcionario que está encargado de la Gestión de TI en atención de sus funciones.

El Manual de Organización de Centros de Gestión Informática, establece en el apartado 5.5.2 Política de estructura organizacional, entre otros aspectos, lo siguiente:

> "***El trabajo se organizará por procesos****, con funcionarios capacitados para el trabajo en equipo y desempeño funcional" (lo resaltado no corresponde al original).*
>
> Adicionalmente, en cuanto al soporte administrativo de los Centros de Gestión Informática el citado manual indica *"realizar otras funciones administrativas propias de su ámbito de competencia, de acuerdo con los requerimientos de la organización y de las autoridades superiores, con el fin de cumplir los objetivos establecidos*".

El Ing. Adrián Campos Rojas encargado de Gestión Informática del Área Salud Heredia-Virilla, indicó[1] que no están definidos ni oficializados los procesos sustantivos, además indicó que las acciones que ejecuta entre otras son:

- Soporte Usuarios.
- Instalaciones de Software institucional y permitido.
- Soporte Hardware (computadoras, impresoras, UPS).
- Bases de datos locales (SIFA, SIGNOS, SIFS, SIES, Marcas de recursos humanos de funcionarios.
- Administración de inventario de stock de repuestos.
- Participación técnica en los procesos de adquisiciones de equipos y servicios de TI.
- Administración y soporte de redes de comunicaciones.
- Administración de usuarios de sistemas institucionales.

Al respecto, la Licda. Mayra Arce Miranda, Administradora del Área de Salud indicó[2] que se elaboró la plantilla de riesgos para todas las áreas de la administración, en la cual se identifican los procesos sustantivos.

Además, detalló que las funciones del Ing. Campos Rojas como responsable de gestión de TI son entre otras el mantenimiento preventivo y correctivo equipos, dar soporte a los usuarios de todos los sistemas institucionales, administrar las redes de comunicaciones y datos y liderar las gestiones de continuidad de Tecnologías de Información y Comunicaciones.

Adicionalmente, el Dr. Gilberto Marín Carmona, Director Médico del Área de Salud, manifestó[3] que no se han definido los procesos sustantivos ni se tienen formalmente documentados.

Se considera que tanto, la Administración como la Dirección Médica del Área de Salud han definido de manera informal actividades y funciones para el encargado de Gestión Informática, las cuales no han sido formalizadas en un manual o documento que establezca con claridad los procesos a cargo de este funcionario en materia de TIC.

La carencia de definición, documentación y aprobación de los procesos sustantivos que son responsabilidad del encargado de Gestión Informática debilita la ejecución de tareas técnicas y administrativas tales como la elaboración de estudios de necesidades, actualización de inventarios, elaboración de planes de capacitación, valoración de riesgos, entre otros, al destinar la mayoría de los recursos y el tiempo laboral en la atención soporte a usuarios.

[1] En entrevista escrita del 3 de junio 2020.
[2] Mediante entrevista escrita del 4 de junio 2020
[3] En Entrevista escrita del 5 de junio 2020

1.2 Planificación Anual Operativa de Gestión de Tecnologías de Información y Comunicaciones

Se determinó que el Ing. Adrián Campos Rojas, encargado de Gestión Informática del Área de Salud Heredia-Virilla no dispone de Planificación Anual Operativa, mediante la cual se establezcan los procesos sustantivos y actividades estratégicas a ejecutar en el periodo de un año, así como las metas o indicadores que permitirán dar seguimiento a lo planificado.

El Manual de Organización de Centros de Gestión Informática define como parte de las acciones por ejecutar, en el apartado de Soporte Administrativo lo siguiente:

> "*Dirigir, coordinar, supervisar y evaluar las actividades sustantivas asignadas, a partir de las políticas, la normativa vigente, **el plan operativo**, el presupuesto, las actividades sustantivas asignadas, los sistemas de información existentes, el análisis de los resultados, las instrucciones de nivel superior, entre otros aspectos, con el fin de detectar desviaciones, corregirlas con oportunidad y lograr la eficiencia y eficacia en el desarrollo de la gestión.*
>
> *(…)*
>
> ***Participar en la formulación del plan operativo** y el presupuesto, de conformidad con las políticas y las normas institucionales vigentes en la materia, los lineamientos establecidos y la estructura por productos y procesos aprobada, con el propósito de definir los objetivos y las metas de trabajo a desarrollar durante el periodo y determinar los recursos necesarios para otorgar los servicios en forma eficiente y eficaz.*
>
> *(…)*
> *Monitorear el cumplimiento de los objetivos y las metas planificadas, mediante la revisión y el análisis del desarrollo de la gestión, con el propósito de tomar las acciones requeridas para el cumplimiento efectivo de las responsabilidades asignadas." (lo subrayado no corresponde al original)*

Al respecto, el Ing. Campos Rojas indicó[4] que no elabora planificación anual para la Gestión de Tecnologías de Información en la cual se incluyan las acciones estratégicas, procesos sustantivos, metas e indicadores de cumplimiento, por su parte, el Dr. Gilberto Marín Carmona, Director General y la Licda. Mayra Arce Miranda, Administradora, refirieron[5] desconocer que dicho proceso de sea realizado por el encargado de TIC.

La atención compartida de las responsabilidades de registro y control de activos y gestión de tecnologías de información por parte del Ing. Campos Rojas provoca una división del tiempo laboral que no está claramente definida, de forma tal que las acciones diarias a ejecutar dependen del nivel de urgencia que se enfrente, por ejemplo si se reciben activos producto de un proceso de adquisición, deben dejarse de lado las actividades de TIC, esta situación limita la posibilidad de desarrollar aspectos de carácter administrativo como la Planificación Anual Operativa o el establecimiento de metas para un periodo especifico.

La ausencia de Planificación Operativa que incluya elementos como actividades estratégicas, metas y objetivos a cumplir, no permite determinar si los recursos disponibles para otorgar los servicios de TIC son utilizados de forma eficiente y efectiva, dado que la mayoría de los esfuerzos están destinados a la atención de solicitudes de soporte técnico. Además de carecer de una herramienta que permita a la administración determinar posibles desviaciones en la obtención de los objetivos planteados y corregirlos oportunamente.

[4] En entrevista escrita del 3 de junio 2020.
[5] Mediante entrevistas escritas del 4 y 5 de junio 2020 respectivamente

1.3 Sobre el Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones

Se determinó que el Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones elaborado por el encargado de TIC en el Área de Salud Heredia-Virilla presenta oportunidades de mejora en aspectos tales como análisis de vigencia de los riesgos incluidos y carencia de ejecución de ensayos programados.

Al respecto, los riesgos incluidos en el Plan de Continuidad de la Gestión TIC son: falla de fluido eléctrico, en hardware, en software, comunicaciones, desactualización de virus, robo de equipo, falta de recurso humano e incendio, los cuales están calificados por impacto, probabilidad y exposición al riesgo según se muestra seguidamente:

Cuadro 1
Clasificación de Riesgos Plan de Continuidad de la Gestión TIC
Área de Salud Heredia-Virilla

Riesgo	Impacto	Probabilidad	Exposición al riesgo	Evaluación de controles existentes	Nivel de riesgo
	Clasificación				
Falla de Fluido Eléctrico	A	M	A	SI	A
Falla en Hardware	A	M	A	SÍ	A
Falla en Software	A	M	A	SI	A
Falla en comunicaciones	A	M	A	NO	A
Desactualización de Antivirus	A	M	M	SI	M
Robo Equipo Informático	A	M	M	SI	M
Falta de Recurso Humano para sustituciones	A	M	M	SI	M
Incendio	A	M	M	NO	M

Fuente: Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, Área de Salud Heredia-Virilla, Pág. 12.

No obstante, se evidenció la ausencia de un proceso de valoración de la vigencia de los riesgos incluidos en el plan de continuidad.

Aunado a lo anterior, se programaron ensayos[6] de los procedimientos de recuperación en caso de materializarse los riesgos de fallas en fluido eléctrico, software e incendios, según se muestra seguidamente:

[6] Los ensayos del PCTIC tiene como finalidad asegurar la viabilidad de las acciones propuestas con el objetivo de asegurar razonablemente la continuidad de la gestión TIC. Adicionalmente, todo ensayo debe ser considerado como una oportunidad para entrenar al personal, tanto en la forma de actuar ante la situación de emergencia como en los procedimientos de recuperación establecidos.

Cuadro 2
Programación ensayos Plan de Continuidad de la Gestión TIC
Área de Salud Heredia-Virilla

Tipo de ensayo	Febrero	Mayo	Noviembre
Falla en Fluido eléctrico	X		
Falla en Hardware		X	
Falla en Software			X

Fuente: Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, Área de Salud Heredia-Virilla, Pág. 52

Sin embargo, a pesar de lo indicado en el cuadro 2 no se realizaron los ensayos planificados para los meses de febrero y mayo de 2019; esto toma relevancia al verificar que se generó una falla en fluido eléctrico el 5 de junio 2019 en el Ebáis de Guararí, ante lo cual se ejecutaron los procedimientos de recuperación, cuyos resultados fueron incluidos en el PCTIC en la plantilla denominada "Ensayo del Plan (PTC017)".

Las Normas de Control Interno para el Sector Público, Capítulo III, Sobre Normas de Valoración del Riesgo en su apartado 3.1 "Valoración de Riesgo", establecen lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar,* ***verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional****, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure."*

Las Políticas de Seguridad Informática institucionales (octubre 2007) establecen en su apartado 10.14 *Política para la elaboración de Planes de Continuidad de la Gestión*, lo siguiente:

> *"Los Planes de Continuidad de la Gestión,* ***deben mantenerse en vigencia y transformarse*** *en una parte integral del resto de los procesos de administración y gestión.*
>
> *La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. (…)".*

Las Normas Institucionales en TIC en el apartado 1.5 Continuidad de los Servicios de Tecnologías de Información, mencionan lo siguiente:

> *"Toda unidad de trabajo debe garantizar una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios internos y externos. Para ello se* ***deben elaborar, actualizar, divulgar y aprobar en los niveles correspondientes el plan de continuidad*** *en las unidades de trabajo que utilicen para su funcionamiento TI.* ***Estos planes deben estar documentados, aprobados por la autoridad correspondiente y puestos a prueba,*** *todo ello, según lo dispuesto en Guía para Elaborar Planes de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones emitido por la Subárea de Continuidad de la gestión TIC".*

El Manual para elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones de la DTIC[7], en el apartado Análisis de Riesgo establece:

[7] Dirección de Tecnologías de Información y Comunicaciones.

"(…)

La actualización de este análisis deberá realizarse al menos una vez al año o cuando las condiciones en el negocio así lo obliguen."

Adicionalmente, el citado Manual en el apartado Mejora Continua establece:

"Revisión constante. El coordinador del plan de continuidad será el responsable por mantener una vigilancia constante sobre el negocio y sobre TI, para identificar eventuales cambios que fuercen a un proceso de actualización de los planes de continuidad y recuperación."

En relación con la valoración en la vigencia de los riesgos, el Ing. Adrián Campos Rojas, manifestó[8] que anualmente se efectúa una evaluación de los riesgos para verificar su actualidad, no obstante, no se dispone de un control de las modificaciones efectuadas. En relación con la ausencia de ensayos indicó que no se han efectuado dado las múltiples tareas que debe atender; además, recientemente la sede del área inició la atención en segundo turno, lo que a su criterio complica aún más realizar esta actividad, pues no se puede detener el servicio de atención a los usuarios.

El Dr. Marín Carmona mencionó[9] que sí conoce los riesgos, pero no los maneja al detalle.

Adicionalmente, recordó que está incluido el tema de soporte eléctrico por medio de la compra de una planta que permita mantener los servicios cuando no falte el fluido, dado que el servidor de datos al que se conectan los Ebáis está ubicado en esta sede y si no se tiene electricidad se corta la conexión con esas unidades externas.

Además, la Licda. Mayra Arce Miranda, Administradora manifestó[10] que desconoce los riesgos incluidos en el Plan de Continuidad de TI, por lo que no puede indicar que se evaluaran para determinar su vigencia.

La ausencia de mecanismos o procedimientos que permitan garantizar un proceso de revisiones periódicas de los riesgos identificados para la plataforma de tecnologías de información y comunicaciones del Área de Salud Heredia-Virilla, está causada primordialmente por la necesidad de fortalecer los procedimientos de gestión administrativa que permitan cumplir de manera eficiente la prestación de servicios TIC a los clientes internos facilitando de esta manera la atención de los asegurados en un ambiente de mayor seguridad.

Lo descrito podría elevar el nivel de vulnerabilidad de los componentes TIC ante nuevas amenazas o riesgos que no se han considerado relevantes tales como ataques a las redes de datos, sustracción de información sensible, daños a componentes de red, ataques físicos a los equipos, entre otras; situación que debería subsanarse mediante una evaluación periódica de los factores de riesgo ambientales o sistemáticos que eventualmente podrían materializarse en el Área de Salud.

Aunado a lo anterior, al no efectuar los ensayos planificados se carece de conclusiones que permitan determinar sobre aspectos como corrección o ampliación de la información, a partir de los resultados obtenidos en los ensayos, nuevos elementos de riesgo identificados tales como personal, documentación o herramientas no ubicadas o no identificadas correctamente; además al no tenerse certeza sobre la eficiencia de los procedimientos definidos para la atención de los riesgos y de los eventuales ajustes que se requieran en tiempo, costo y dificultades de la aplicación de los procedimientos de recuperación.

1.4 Sobre los indicadores de gestión del Centro de Gestión Informática

Se evidenció que la administración del Área de Salud Heredia-Virilla no dispone de indicadores de gestión que permitan efectuar una medición del desempeño del encargado de Gestión Informática.

[8] En entrevista escrita del 3 de junio 2020.
[9] En entrevista escrita del 5 de junio 2020
[10] En entrevista escrita del 4 de junio 2019.

El Manual de Organización de Centros de Gestión Informática define como parte de las acciones por ejecutar, en el apartado de Soporte Administrativo:

> *"(…)*
>
> *Monitorear el cumplimiento de los objetivos y las metas planificadas mediante la revisión y análisis del desarrollo de la gestión, con el propósito de tomar las acciones requeridas para el cumplimiento efectivo de las responsabilidades asignadas"*

El Ing. Campos Rojas, encargado de Gestión informática del Área de Salud Heredia-Virilla manifestó[11]:

> *"(…) algunas de las formas en las cuales la administración puede medir el cumplimiento de mis labores están determinadas por las eventuales quejas que desde los servicios puedan darse, o en que eventualmente no se alcancen las metas de compras y renovaciones de equipos que se plantean a principio del periodo. Pero desconoce de cuales indicadores de gestión utiliza la administración para medir sus labores."*

Al respecto la Licda. Mayra Arce Miranda, Administradora indicó[12] que no conoce que se establecieran indicadores de gestión para medir el cumplimiento de metas del encargado de CGI, adicionalmente el Dr. Gilberto Marín Carmona, Director Médico mencionó[13] que no se han establecido indicadores para la gestión que lleva a cabo el Ing. Campos Rojas.

La ausencia de indicadores de gestión formalmente definidos podría comprometer la entrega de información como insumo para la planificación de las actividades, así como el aporte de elementos para que el jerarca y los titulares subordinados estén en capacidad de revisar, evaluar y ajustar periódicamente los procesos de planificación operativa en materia de tecnologías de información y comunicaciones.

2. GESTIÓN TÉCNICA DEL CENTRO DE GESTIÓN INFORMÁTICA

Se evidenciaron debilidades en el desarrollo de la gestión técnica en materia de gestión de tecnologías de información y comunicaciones, en aspectos relacionados con: desarrollo e implementación de protocolos de seguridad para el aseguramiento de los activos informáticos, elaboración y desarrollo de planes de capacitación, registro de atención de incidencias y protocolos de aseguramiento de respaldo de bases de datos locales, según se detalla seguidamente:

2.1 Desarrollo e implementación de protocolos de seguridad para los activos informáticos

Se evidenció que la administración del Área de Salud Heredia-Virilla no ha desarrollado, documentado ni formalizado los protocolos de seguridad para los activos informáticos, entre los que se encuentran computadoras, impresoras, redes y equipos de comunicación de datos y servidores, entre otros.

La Ley General de Control Interno 8292, en su artículo 8 "Concepto de Sistema de Control Interno", establece lo siguiente:

> "*Para efectos de esta Ley, 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, irregular o acto ilegal."*

[11] En entrevista escrita del 3 de junio 2020
[12] En entrevista escrita del 4 de junio 2020
[13] En entrevista escrita del 5 de junio 2020

El Manual de Organización de Centros de Gestión Informática define como parte de las acciones por ejecutar, en el apartado de Gestión Técnica, lo siguiente:

> "*Documentar e implementar la política de seguridad de la información, con base en la regulación y la normativa vigente, con el objetivo de lograr confiabilidad: física y ambiental, en las operaciones y las comunicaciones, el control de acceso, la implementación, el mantenimiento de software e infraestructura tecnológica y la continuidad de los servicios, entre otros aspectos.*"

El Ing. Campos Rojas, encargado de Gestión Informática, indicó[14]:

> *"El caso del hardware, se tiene establecido que el servicio de seguridad debe verificar que el funcionario que tiene el equipo cuente con la boleta de permiso de salida debidamente autorizada por la jefatura correspondiente.*
>
> *En software y acceso a la información, se ha implantado un protocolo con la asignación de protocolos de administradores de seguridad de los sistemas, en el cual se dan permisos según las solicitudes de las jefaturas, como administrador local cuento con perfil en todos los sistemas, en el caso de SIES la Dra. María Fernanda Villaseñor Carvajal, en SIAC el Sr. Juan Pablo Arias Barrantes quien funge como administrador de agendas y en el SIFF la Dr. Idianey Ortega Bustos.*
>
> *En el caso de licencias no existen medios físicos que custodiar y en el caso de acceso a los respaldos se cuenta con respaldos programados en el SQL Server, tenemos acceso a los respaldos únicamente mi persona un funcionario de farmacia y uno de presupuesto para poder tener tres ubicaciones independientes. También tengo un respaldo que se envía a la DRIPSSCN."*

Al respecto, la Licda. Mayra Arce Miranda, Administradora, manifestó[15] que se dispone de un control de salidas de activos, el cual ha sido comunicado en la contratación por terceros de vigilancia y a las jefaturas de servicios.

La situación descrita implica debilidades en las acciones relacionadas con la protección de los diversos recursos informáticos, elevando el nivel de exposición al riesgo de los elementos que componen la infraestructura TIC de la unidad, esta condición se presenta por la inacción de la administración y el encargado de TI, quienes han establecido procedimientos de seguridad de los activos informáticos, no obstante, no han procedido a su documentación, formalización y comunicación a los funcionarios del Área de Salud.

La ausencia de documentación, oficialización y comunicación de los protocolos que describan los procesos de implementación y cumplimiento de controles de seguridad, aumenta la vulnerabilidad de los componentes de la infraestructura de TIC del área, elevando las posibilidades de sufrir entre otros eventos tales como sustracciones, sabotajes, intrusiones malignas u otros que comprometan la prestación de los servicios de TI y por ende la continuidad en la atención a los asegurados.

2.2 Capacitación en Tecnologías de Información y Comunicaciones a funcionarios del Área de Salud y del Centro de Gestión Informática

Se determinó que la administración del Área de Salud Heredia-Virilla carece de un plan de capacitación en temas relacionados con TIC tanto para el encargado de la gestión informática como para los funcionarios del Área, con la finalidad de fortalecer y ampliar los conocimientos en relación con las funciones que ejecutan. Además, no se evidencia la atención de labores sustantivas de capacitación y asesoría a los usuarios de la plataforma tecnológica.

[14] En entrevista escrita del 3 de junio 2020
[15] En entrevista escrita del 4 de junio 2020

El Manual de Organización de Centros de Gestión Informática en el apartado 5.5.4 "Política de Recursos Humanos", establece que:

> *"La formación, la capacitación y la actualización profesional del recurso humano serán elementos básicos para solventar las debilidades detectadas y fortalecer las habilidades y destrezas requeridas por la organización".*

El citado manual refiere además, en relación con la capacitación y asesoría de los usuarios de la plataforma de TI en el apartado de Conceptualización del Área de Gestión de Tecnologías de Información, lo siguiente:

> *"Otorga la capacitación y la asesoría para la solución de problemas operativos, que se les presentan a los usuarios finales en la utilización de la tecnología de información".*

Adicionalmente, como parte de la Gestión Técnica de los Centros de Gestión Informática, en ese documento se indica:

> *"Capacitar y asesorar a los usuarios en el uso de los sistemas y de las aplicaciones en operación, de acuerdo con las necesidades específicas, las políticas y los manuales técnicos vigentes, con la finalidad de lograr la operación efectiva y la confiabilidad de la información.*
>
> (…)
>
> *Asesorar y capacitar a los funcionarios para que se cumplan las regulaciones relacionadas con la seguridad. confiabilidad y riesgos asociados en tecnologías de información y comunicaciones, de acuerdo con la normativa establecida, con el fin de reducir los riesgos de error humano, sustracción, fraude o uso inadecuado de los recursos tecnológicos".*

El Ing. Campos Rojas, encargado de TIC en el Área de Salud Heredia-Virilla, indicó[16] que no se tienen planes de capacitación para fortalecer el conocimiento en las funciones que ejecuta, además mencionó que tiene necesidad de fortalecer áreas relacionadas con la administración de bases de datos y funcionamiento de impresoras entre otros, estas necesidades las ha manifestado en las evaluaciones del desempeño anuales.

Respecto a la capacitación y asesoría a los usuarios el Ing. Campos Rojas indicó[17]:

> *"(…) que dado el limitado tiempo con que cuenta no puede realizar actividades de capacitación a usuarios finales."*

La Licda. Mayra Arce Miranda, Administradora, refirió[18] que no se dispone de planes de capacitación en temas de tecnologías de información y comunicaciones para los funcionarios del Área de Salud.

La capacitación continua permite fortalecer las competencias de los funcionarios, este proceso resulta de vital importancia en las áreas de tecnologías de información y comunicaciones cuyo ritmo de cambio e innovación es constante.

Aunado a lo anterior, la ejecución de las funciones propias de Tecnologías de Información y Comunicaciones requiere conocimientos relacionados con administración de servidores locales, continuidad del negocio y recuperación de servicios, atención de solicitudes de soporte técnico de los clientes internos, configuración de impresoras y dispositivos de comunicación, entre otras, por lo que requiere de capacitaciones que les permitan mantener actualizados sus conocimientos técnicos.

[16] En entrevista escrita del 3 de junio 2020
[17] En entrevista escrita del 3 de junio 2020
[18] En entrevista escrita del 4 de junio 2020

Al respecto, el incumplimiento de las tareas sustantivas en torno a brindar asesoría y capacitación a los usuarios en materia de TIC podría materializar riesgos relacionados con el conocimiento y aplicación de las normas establecidas institucionalmente en temas como seguridad informática o utilización de las herramientas diseñadas para la atención oportuna de los asegurados.

2.3 Sobre la gestión de las solicitudes de soporte técnico

En el Área de Salud Heredia-Virilla no se ha establecido un procedimiento formal para la atención de solicitudes de soporte técnico, dado que el encargado de gestión informática recibe solicitudes por medio de llamadas telefónicas, correos electrónicos o verbalmente.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República, establecen en el inciso 4.2 "Administración y operación de la plataforma tecnológica", que:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: (…) Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas (…)".*

Al respecto el Ing. Campos Rojas, indicó[19]:

> *"(…) las incidencias se reciben por medio de correo electrónico, llamadas o vista de los funcionarios a la oficina, en caso de ser un evento de alguno de los lugares fuera de la sede se valora el acceso remoto al equipo para la atención del incidente y se realizan los ajustes o cambios solicitados por el usuario, ya sea instalación de software o configuraciones de impresoras o de escritorio para el uso del funcionario, se si determina que es problema de hardware se programa una visita al sitio, se coordina con transportes el traslado al sitio.*
>
> *Si el incidente es en la sede, se procede a realizar la inspección en el sitio, en caso de problemas de comunicaciones, se hacen pruebas de conectividad de mi equipo al sitio para determinar la fuente del problema, en caso de necesario se abre un incidente con mesa de servicios para la atención del caso con el proveedor del servicio. En el caso de los equipos EDUS-ICE se llena un formulario y se envía a la mesa de servicios con copia a la Ing. Ana Elizondo (DRIPSSCN) para la atención del caso.".*

Además, añadió que no se ha documentado ni formalizado el procedimiento de atención de las incidencias, no obstante, los usuarios saben cómo localizarlo y solicitar que se atiendan sus requerimientos. Adicionalmente, señaló que en promedio se atienden 6 solicitudes diarias, sin embargo, únicamente cuenta con una platilla en Excel para el registro de los casos, en la cual no se incluye de manera inmediata la información de cada atención.

Lo descrito, dificulta tener claridad sobre la atención real de las solicitudes de soporte técnico que se ejecutan en el Centro de Gestión Informática, de forma tal que se desconoce no solo el tiempo dedicado a esta actividad, si no el peso real que debe destinarse a este proceso del CGI.

2.4 Sobre el resguardo de respaldos de bases de datos locales

Se evidenció que los respaldos de bases de datos del Área de Salud Heredia-Virilla se resguardan en equipos de funcionarios encargados de los procesos en los cuales se utiliza esa información, sin disponer de protocolos que permitan establecer las responsabilidades que les competen en temas relacionados con la seguridad y uso inadecuado de los datos almacenados.

[19] En entrevista escrita del 27 de marzo 2019.

Las Políticas de Seguridad Informática Institucionales en su apartado 10.10 PSI-UAR-010 "Política Realización de Respaldos", establece:

> *"La realización periódica de respaldos de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de los funcionarios de la CCSS, es de gran importancia para brindar continuidad de los servicios. Por lo tanto todas las unidades de la institución deben elaborar un plan de recuperación y respaldo de información, donde los respaldos deberán realizarse periódicamente conforme las características de los equipos, las aplicaciones y los datos asociados. El plan de recuperación y respaldo de la información debe contemplar la realización de pruebas continuas para asegurarse que los respaldos estén correctamente ejecutados y* ***deben almacenarse en un lugar seguro y lejano de la fuente de información original.****"*

Al respecto el Ing. Campos Rojas indicó[20]:

> *"En el caso de los respaldos que son custodiados por los funcionarios de farmacia y presupuesto no se han documentado las responsabilidades que competen en el tema de seguridad en el uso de la información, de modo que no se tiene documentación que permita responsabilizarlos en caso de perdida, daño o uso inadecuado de las bases de datos que custodian.*
>
> *"(...) En el caso de los funcionarios mencionados no se ha documentado la responsabilidad del manejo de los aspectos de seguridad o de los respaldos correspondientes."*

La ausencia de protocolos de seguridad relacionados con la responsabilidad de los funcionarios que resguardan respaldos de bases de datos locales obedece a que a nivel del centro de salud no se han establecido actividades de control que permitan garantizar que las tecnologías de información se acompañen de una gestión efectiva por parte de los involucrados en el proceso.

Lo descrito eleva los riesgos relacionados con resguardos adecuados de la información, además de la eventual sustracción y uso de datos institucionales por parte de terceros; además, se genera la posibilidad de utilización indebida de esos datos por parte de los funcionarios que los custodian al no disponer de responsabilidades documentadas sobre su almacenamiento, resguardo y uso.

CONCLUSIONES

La Gestión de Tecnologías de Información y Comunicaciones debe constituirse en una herramienta de apoyo a los procesos sustantivos de la institución, mediante la ejecución de acciones que permitan asegurar la información y los componentes de la plataforma de TI de cada unidad, elementos que facilitan la toma de decisiones para una mejor prestación de servicios a los asegurados.

En relación con la gestión administrativa del encargado de gestión informática del Área de Salud Heredia-Virilla, se evidenciaron aspectos sujetos de mejora como la ausencia de elementos que permitan establecer con claridad los objetivos y metas planteados en TIC, tales como la carencia de definición de procesos sustantivos, la ausencia de planificación anual operativa y de indicadores de gestión que permitan medir el cumplimiento y el avance de lo planteado en esta materia.

Además, en lo referente a riesgos incluidos en el Plan de Continuidad de la Gestión TIC, no se han efectuado acciones que permitan determinar si los actuales aún son vigentes, o si eventualmente se requieren modificaciones para que contemplen los cambios constantes de la zona geográfica en la cual se ubican la sede del Área de Salud y los Ebáis desconcentrados.

[20] En entrevista escrita del 3 de junio 2020

Se evidenciaron oportunidades en el desarrollo de la gestión técnica en materia de gestión de tecnologías de información y comunicaciones, en aspectos relacionados con: desarrollo e implementación de protocolos de seguridad para el aseguramiento de los activos informáticos, elaboración y desarrollo de planes de capacitación, registro de atención de incidencias y protocolos de aseguramiento de respaldo de bases de datos locales, según se detalla seguidamente:

Respecto a la gestión técnica, es necesario indicar que no se han desarrollado protocolos de seguridad específicos para el aseguramiento de los activos informáticos elevando el riesgo de sustracciones, acceso a no autorizado a redes, entre otros. Adicionalmente, no se han desarrollado programas de capacitación para el encargado de TIC que permita facilitar el crecimiento en las habilidades técnicas requeridas para la atención de las actividades sustantivas que están a su cargo. Igualmente se carece de programas de capacitación para los usuarios de las TIC del Área de Salud, que permitan refrescar o ampliar conocimientos que faciliten sus funciones tanto en las aplicaciones institucionales como en temas relacionados con el uso de las tecnologías de información y comunicaciones.

Aunado a lo anterior, al permitir el resguardo y custodia de respaldos de bases de datos institucionales sin contar con un protocolo que permita identificar a los funcionarios, así como sus responsabilidades en la custodia de esos datos, ni de responsabilizarlos en caso de sustracciones o usos inadecuados, eleva el riesgo de una eventual utilización indebida o sustracción de información lo que provocaría daños tanto a la imagen institucional como a su patrimonio.

RECOMENDACIONES

AL DR. GILBERTO MARÍN CARMONA, DIRECTOR MÉDICO DEL ÁREA DE SALUD HEREDIA VIRILLA O QUIEN EN SU LUGAR OCUPE EL CARGO

1. Definir y documentar en coordinación con la Administradora y el encargado de Gestión Informática, de conformidad con hallazgo 1.1 referente a la definición de los procesos de TIC, los procesos sustantivos que deben ser atendidos por el Centro de Gestión Informática de esta unidad.

Para acreditar el cumplimiento de esta recomendación, deberá aportarse en un plazo de 6 meses a partir del recibido del presente informe, la documentación que respalde la identificación de los procesos sustantivos, debidamente aprobados por parte de esa Administración.

2. Definir y desarrollar en conjunto con la Administradora y el encargado de gestión informática los objetivos y actividades a incluir en la planificación anual del CGI, así como los metas que permitan brindar seguimiento a lo planificado, de conformidad con el hallazgo 1.2 referente a la ausencia de planificación anual.

Para acreditar el cumplimiento de esta recomendación, deberá aportarse en un plazo de 6 meses a partir del recibo del presente informe, el respaldo documental del análisis realizado así como de los objetivos, actividades y metas incluidos en la planificación del CGI.

3. Realizar, en conjunto con la Administradora y el encargado de Gestión Informática de conformidad con el hallazgo 1.3 referente a la vigencia de los riesgos incluidos en el Plan de Continuidad de la Gestión y la ausencia de ensayos las siguientes acciones:

a. Revisar la vigencia de los riesgos incluidos en el Plan de Continuidad.
b. Garantizar la ejecución de los ensayos programados y la documentación de los resultados.

Para acreditar el cumplimiento de la recomendación deberá aportarse en un plazo no mayor a 6 meses luego de la recepción de este informe, el análisis de la vigencia de los riesgos incluidos en el plan de continuidad (inciso a) y los resultados de los ensayos efectuados (punto b).

4. Ejecutar en conjunto con la Administradora, de conformidad con el hallazgo 1.4 referente a la ausencia de indicadores de gestión del encargado de TIC, lo siguiente:

a. Establecer los indicadores de gestión requeridos para evaluar el cumplimiento de las labores sustantivas que debe ejecutar el encargado de Gestión Informática.

b. Implementar mecanismos de control dirigidos a garantizar la supervisión y análisis del comportamiento de los indicadores de gestión definidos.

Para acreditar el cumplimiento de esta recomendación, deberá aportarse evidencia en un plazo de 6 meses a partir del recibo del presente informe, de los indicadores de gestión (inciso a) y para la atención del apartado b) evidencia de la implementación de los mecanismos de control y supervisión.

A LA LICDA. MAYRA ARCE MIRANDA, ADMINISTRADORA DEL ÁREA DE SALUD HEREDIA-VIRILLA O QUIEN EN SU LUGAR OCUPE EL CARGO

5. Implementar en coordinación con el encargado de gestión TIC los protocolos de seguridad para los elementos que conforman la infraestructura de TIC en esa área de salud, de conformidad con el hallazgo 2.1 referente a la ausencia de protocolos de seguridad para los activos informáticos.

Para acreditar el cumplimiento de la recomendación se deberá aportar en un plazo de 6 meses a partir del recibo del informe, la documentación que respalde el desarrollo e implementación de los protocolos de seguridad.

6. Elaborar un plan de capacitación dirigido a fortalecer los conocimientos y capacidades de los funcionarios del área de salud en tecnologías de información, en aspectos sustantivos como administración de servidores, usuarios, redes e infraestructura tecnológica, soporte técnico, entre otros, el cual deberá ser incorporado en el Plan de Capacitación y Formación de esa unidad, así como para los usuarios finales, de conformidad el hallazgo 2.2 referente a las necesidades de capacitación en TIC de los funcionarios.

Para acreditar el cumplimiento de esta recomendación deberá remitirse en un plazo de 6 meses a partir del recibo de este informe, la documentación que respalde la realización del plan solicitado y su inclusión en el plan de capacitación y formación.

7. Establecer un procedimiento para la atención de solicitudes de soporte técnico, en el cual se considere la utilización de alguna de las herramientas institucionales diseñadas para el control y registro de actividades de soporte de TIC, de conformidad con el hallazgo 2.3, sobre la ausencia de procedimientos formales para la atención de solicitudes de soporte técnico.

Para acreditar el cumplimiento de esta recomendación deberá aportarse evidencia del procedimiento, su socialización y efectiva implementación en un plazo de 6 meses a partir recibido el presente informe.

8. Establecer, en coordinación con el encargado de Gestión de Tecnologías de Información y Comunicaciones de conformidad con lo descrito en el hallazgo 2.4 sobre resguardos de bases de datos locales, un procedimiento que permita asegurar que los respaldos sean almacenados por los funcionarios adecuados y en lugares que se ajusten a lo establecido en la normativa institucional y las buenas prácticas en la materia, con la finalidad de asegurar el buen uso de la información institucional y las posibles responsabilidades que se generen en caso de sustracciones o uso inadecuado.

Para acreditar el cumplimiento de esta recomendación deberá aportarse evidencia del procedimiento, su socialización y efectiva implementación en un plazo de 3 meses a partir recibido el presente informe.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente informe se comentaron con el Dr. Gilberto Marín Carmona, Director Médico y la Licda. Mayra Arce Miranda, Administradora, funcionarios del Área de Salud Heredia-Virilla, quienes hicieron los siguientes comentarios:

El Dr. Gilberto Marín Carmona, Director Médico, indicó que dadas las condiciones actuales de la atención del Covid-19 se tienen responsabilidades tales como la reconversión de la atención de la consulta, así como de la realización de testeos masivos y de solución de las solicitudes que se reciban del nivel superior en esta materia, de forma tal que se debe considerar que los plazos de atención podrían ser más extensos de nuestra parte.

La Licda. Mayra Arce Miranda, Administradora, indicó que se debe considerar que el Área de Salud únicamente tiene un funcionario a cargo de los procesos de TIC, por lo cual es probable que ante el aumento de la digitalización de los procesos, también se tengan retrasos en la atención de las recomendaciones del informe.

ÁREA DE GESTIÓN OPERATIVA

ALEXANDER ARAYA MORA (FIRMA)
Firmado digitalmente por ALEXANDER ARAYA MORA (FIRMA)

Br. Alexander Araya Mora
Asistente de Auditoría

MIGUEL ANGEL SALVATIERRA ROJAS (FIRMA)
2020.07.10 10:04:00 -06'00'

Ing. Miguel Ángel Salvatierra Rojas
Jefe de Subárea

MASR/AAM/ams

Referencia: (ID-36067)