CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

AGO-37-2019
28-05-2019

RESUMEN EJECUTIVO

El estudio se realizó de conformidad con el Plan Anual de Trabajo 2019 del Área Gestión Operativa, apartado actividades programadas, con el propósito evaluar la gestión en tecnologías de información en el Área de Salud Cariari.

Los resultados del presente informe evidencian debilidades relacionadas con la gestión administrativa en aspectos como: definición de los procesos sustantivos que ejecuta, identificación de los riesgos incluidos en Plan de Continuidad de la Gestión, así como en la elaboración del Plan Anual Operativo y su seguimiento; además de carecer de indicadores de gestión que permitan valorar el alcance de las acciones que ejecutan los funcionarios encargados 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, la carencia de elementos de seguridad física en el CGI podría provocar eventualmente la materialización de riesgos relacionados con acceso a los servidores, ejecución de labores de revisión y mantenimiento de equipos, control de inventarios de suministros y activos entre otros.

Adicionalmente, se ubicaron equipos de cómputo nuevos y usados (monitores, UPS y otros) almacenados en el archivo de expedientes del Ebáis de Cariari 1, el cual no cuenta con mecanismos de control de acceso.

Finalmente, el Expediente Digital Único en Salud, no ha sido implementado en su totalidad en el Servicio de Urgencias y en los puestos de visita periódica del área, ocasionando que la información que se genera en esas atenciones no sea incluida en su totalidad en el expediente de cada asegurado que consulta.

En virtud de los resultados se emiten 9 recomendaciones dirigidas a las autoridades del Área de Salud Cariari, con la finalidad de fortalecer los procesos relacionados con gestión administrativa, gestión técnica, seguridad física, e implementación del EDUS.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

AGO-37-2019
28-05-2019

ÁREA GESTIÓN OPERATIVA
AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN EL ÁREA DE SALUD CARIARI

ORIGEN

El presente estudio se realizó en atención al Plan Anual Operativo del Área Gestión Operativa para el 2019, apartado de actividades programadas.

OBJETIVO GENERAL

Evaluar la gestión en tecnologías de información y comunicaciones en el Área de Salud Cariari.

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.

- Comprobar las condiciones de seguridad física de las instalaciones utilizadas por el Centro de Gestión Informática.

ALCANCE

El estudio comprendió la revisión y análisis de las actividades sustantivas propias del Centro de Gestión Informática del Área de Salud durante los años 2017-2018, 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.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

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.
- Análisis de la Autoevaluación de Riesgos del Centro de Gestión Informática del Área de Salud Cariari.
- Verificación de protocolos de seguridad de los equipos.
- Inventario en bodega de stock de dispositivos y componentes.
- Análisis de las condiciones de seguridad física del Centro de Gestión Informática del Área de Salud Cariari.
- Entrevista al Ing. Ángel Ríos Maldonado, Coordinador del Centro de Gestión Informática del Área de Salud Cariari.

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.
- Instructivo que regula los faltantes y sobrantes de activos y suministros en la C.C.S.S, setiembre 2009.

DISPOSICIONES RELATIVAS A LA LEY GENERAL DE CONTROL INTERNO

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:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

"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 (…)".

HALLAZGOS

1. GESTIÓN ADMINISTRATIVA DEL CENTRO DE GESTIÓN INFORMÁTICA DEL ÁREA DE SALUD CARIARI

Se evidenciaron debilidades en la gestión administrativa del Centro de Gestión Informática (CGI) del Área de Salud Cariari en aspectos relacionados con: definición de los procesos sustantivos, identificación de los riesgos incluidos en Plan de Continuidad de la Gestión, debilidades en la elaboración del Plan Anual Operativo y su seguimiento, así como indicadores de gestión, según se detalla seguidamente:

1.1 Definición de los procesos que ejecuta el Centro de Gestión Informática

Se evidenció que el Centro de Gestión Informática del Área de Salud Cariari no ha definido ni documentado formalmente los procesos que debe ejecutar en atención de sus funciones; además el listado de actividades y responsabilidades para cada funcionario de esa unidad no ha sido valorado y aprobado por la jefatura administrativa del Área.

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 Centro 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. Ángel Ríos Maldonado encargado del CGI del Área de Salud Cariari[1], indicó que:

"En ese proceso se han definido las tareas de cada uno y se comunicaron a la administración, para su revisión y aprobación. De forma tal que en este momento tenemos definido las responsabilidades en forma de prosa y no de procesos, a la espera de la aprobación de la dirección administrativa del marco de responsabilidades de cada uno de los funcionarios del CGI."

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

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

Adicionalmente, el Ing. Ángel Ríos Maldonado[2], comunicó la distribución de actividades para cada uno de los funcionarios que laboran en el CGI del Área de Salud Cariari, que se detallan seguidamente:

Cuadro 1
Actividades Centro Gestión Informática
Área de Salud Cariari

Actividades	Coordinador	Operador TIC
Elaboración y Seguimiento del Plan de Continuidad de la Gestión	X	
Realizar control interno para CGI	X	
Realizar Plan Operativo CGI	X	
Realizar planes estratégicos para reemplazo de equipos de cómputo	X	
Elaborar Plan de riesgos bajo metodología SEVRI	X	
Participar en Consejos Administrativos y de Informática	X	
Colaborar y asesorar a los diferentes departamentos y servicios en la metodología de elaboración de documentación solicitados para el desarrollo de proyectos en TIC	X	
Brindar mantenimiento preventivo y correctivo de equipo de cómputo	X	X
Brindar soporte técnico al hardware y software de los equipos y red informática institucional		X
Supervisar y aplicar las políticas de uso de la tecnología de información y comunicaciones de la institución	X	X
Implementar los sistemas y aplicaciones institucionales	X	X
Aplicar las políticas de seguridad informática institucionales	X	X
Aplicar el Plan de Continuidad en los distintos procesos del uso de la red, sistemas y recursos informáticos institucionales	X	X
Administrar las redes estructuradas e inalámbricas de la institución	X	X
Desarrollar procesos para facilitar al usuario el uso o configuración de aplicaciones, sistemas o recursos informáticos	X	X
Desarrollar capacitaciones para los usuarios en el uso de aplicaciones, sistemas o recursos informáticos	X	X
Colaborar con los usuarios en la elaboración de recursos digitales que facilitan el desarrollo de tareas y funciones	X	X
Brindar apoyo para el desarrollo de soluciones informáticas y ofimáticas para los diferentes servicios o departamentos	X	X

Fuente: Encargado de Gestión en Tecnologías de Información y Comunicaciones, Área de Salud Cariari

[2] Mediante correo electrónico del 20 de febrero 2019

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

El Centro de Gestión Informática del Área de Salud Cariari ha establecido una serie de actividades que deben ser atendidas por el personal técnico; no obstante, estas actividades no han sido aprobadas por parte de la jefatura administrativa del área, ocasionando que adicionalmente, no se hayan definido ni documentado los procesos relevantes que se debe ejecutar.

La carencia de definición y aprobación de los procesos que son responsabilidad del Centro de Gestión Informática ocasiona que los recursos disponibles se utilicen principalmente en la atención de las solicitudes de incidencias de soporte técnico, debilitando la atención de otras funciones tales como elaboración de estudios de necesidades, actualización de inventarios, elaboración de planes de capacitación, entre otros.

1.2 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 CGI presenta debilidades relacionadas con los riesgos definidos para esa unidad, tales como: ausencia de análisis de vulnerabilidades de la zona en la que se ubica la sede del área y las edificaciones que albergan los Ebáis, así como valoración de todos los equipos de TIC del área en categoría “no crítico” sin el análisis correspondiente.

Adicionalmente, se verificó que para riesgos de distinta naturaleza se reiteran las acciones a ejecutar durante y después de su manifestación, a pesar de que son eventos completamente diferentes, por ejemplo: desastres naturales, robo, incendios (nivel de riesgo alto), huracán, virus, falla de aire acondicionado y fallo en respaldo, los cuales no necesariamente están asociados a las acciones identificadas, evidenciado que el análisis es insuficiente, según se muestra a continuación:

Cuadro 2
Acciones por ejecutar durante y después de la manifestación de un riesgo
Área de Salud Cariari

Riesgo	Nivel de Riesgo	Acciones por ejecutar durante la manifestación del riesgo	Acciones por ejecutar posterior a la manifestación del riesgo
Desastres Naturales	Medio	Subir a una posición elevada el equipo de cómputo. Desconectar fluido eléctrico de áreas afectadas.	Limpiar y secar el equipo de cómputo. Tomar nota de los equipos dañados. Consultar Póliza de seguro con la administración. Enviar a reparar equipo en garantía.
Robo	Medio		
Incendio	Alto		
Huracán	Medio		
Virus	Medio		
Falla en Aire Acondicionado	Medio		
Fallo en Respaldo	Medio		

Fuente: Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, Área de Salud Cariari.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

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 Normas Técnicas para la Gestión de las Tecnologías de Información de la Contraloría General de la República, en el apartado 1.4.7 Continuidad de los servicios de TI indican que:

"La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."

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".

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

El Manual para elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones de la DTIC[3], en el apartado Análisis de Riesgo establece:

"Busca determinar los eventos y situaciones externas que pueden afectar adversamente a la organización y su infraestructura, tanto por una interrupción como por un desastre, evalúa el daño que dichos eventos pueden causar, y los controles requeridos para prevenir o minimizar los efectos de pérdida potencial. Provee un análisis costo-beneficio para justificar la inversión requerida para mitigar los riesgos identificados.

(…)

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."

Respecto a los riesgos incluidos en el Plan de Continuidad de la Gestión[4], se evidenció la siguiente anotación en la versión 1.8 para el Área de Salud Cariari:

"Los desastres naturales contemplados en esta tabla tienen su origen en base a las reuniones de los CGI que se hacían en la Dirección Regional donde en conjunto definimos algunos factores de riesgo a los que está expuesta la provincia.

Los demás riesgos (Hurtos, fallos en medios de respaldo, fallos de software, fallo eléctrico y ruptura de averías) se basan en los reportes anotados en las boletas de soporte técnico."

Al respecto el Ing. Ángel Ríos Maldonado, encargado del CGI del Área de Salud Cariari[5], indicó que para la definición de los riesgos incluidos en el plan no se utilizó ninguna herramienta técnica, se basó en un análisis de las condiciones propias de la zona en la que se ubica el área.

Respecto a la vigencia de los riesgos el Ing. Ríos Maldonado, manifestó que no se ha aplicado ningún proceso de evaluación que permita valorar si los riesgos incluidos deben ser actualizados de acuerdo con modificaciones ambientales o sociales de la zona, tanto en su definición como en el nivel de riesgo establecido en cada caso.

[3] Dirección de Tecnologías de Información y Comunicaciones.
[4] Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, Área de Salud Cariari, página 19, plantilla: Captura de la Información de Riesgos - ARV001.
[5] En entrevista escrita del 27 de marzo 2019.

Sobre la razón para no incluir como crítico ningún equipo de TI del área de salud el Ing. Ríos Maldonado, indicó que la clasificación se hizo con base en el criterio de que la afectación de los servicios no es total si falla alguno de los equipos, de forma tal que no se consideró que debe darse esa clasificación a alguno de ellos.

Finalmente, en relación con la reiteración de las acciones a ejecutar antes, durante y después de la materialización del riesgo, el Ing. Ríos Maldonado indicó que se debe a una equivocación al momento de desarrollar el Plan de Continuidad de la Gestión.

Lo descrito, muestra la ausencia de mecanismos o procedimientos que permitan garantizar un proceso de revisiones periódicas de los riesgos establecidos para la plataforma de tecnologías de información y comunicaciones del Área de Salud Cariari, al no considerar elementos tales como cambios en el ambiente organizacional que modifiquen los elementos incluidos en el plan (en la plataforma, en los procesos que se ejecutan o en el personal a cargo).

Aunado a lo anterior, no se considera en el análisis de riesgos la extensión y condición geográfica en la que se ubica el área de salud, este elemento introduce un nivel de complejidad en la continuidad de los servicios de TI, al tener sedes de Ebáis ubicadas en lugar alejados y con dificultades de acceso, en los cuales la materialización de un riesgo probablemente ocasione retrasos en la atención de la consulta de los asegurados o la suspensión total.

Es importante señalar, que la reiteración de las acciones a ejecutar antes, durante y después de la materialización de un riesgo expone al personal a cargo a desconocer la forma de proceder ante diversos eventos tales como robo, incendio o inundaciones, elevando las posibilidades de afectaciones económicas y de alteración en la prestación de los servicios de salud.

1.3 Planificación Anual Operativa del Centro de Gestión Informática

El Centro de Gestión Informática del Área de Salud Cariari elabora el documento denominado “Plan Anual Operativo”, mediante el cual establece las actividades a ejecutar en el periodo de un año, así como los indicadores (metas) que permitirán dar seguimiento al plan; no obstante, se incluyen objetivos y actividades que corresponden a la ejecución de actividades propias de la gestión administrativa, entre los que se encuentran: Elaboración de informe de necesidades, elaboración del Plan Anual Operativo, además de otros cuya ejecución no depende de esa dependencia como por ejemplo: asistencia a Consejos Regionales y al Congreso de Tecnologías de Información y Comunicaciones organizado por la DTIC.

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

"*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."

Al respecto el Ing. Ángel Ríos Maldonado indicó que las acciones estratégicas, procesos sustantivos, metas e indicadores que se incluyen en el Plan Anual se definen con base en los planes de años anteriores; además se toman en cuenta tareas que son asignadas por la administración y que no dispone de herramientas administrativas o metodológicas que le permitan establecer los elementos a incluir en la planificación.

La inclusión de actividades que representan acciones propias de la labor de tecnologías de información como parte de los objetivos y metas a desarrollar en la planificación anual, se genera en el desconocimiento de las necesidades que tiene el área de salud en cuanto al desarrollo de la plataforma de TI, además de provocar que la mayoría de los recursos se utilicen en la atención diaria de solicitudes de soporte técnico.

Debilidades en el proceso de planificación generan el riesgo de uso inadecuado de los recursos destinados al desarrollo de las tecnologías de información y comunicaciones en el Área de Salud no se utilicen de manera eficiente y que generen impacto en la prestación de los servicios a los asegurados, dado que se utilizaran en la atención de actividades que deben desarrollarse de manera obligatoria tales como la elaboración de planes y estudios de necesidades.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

1.4 Sobre los indicadores de gestión del Centro de Gestión Informática.

Se evidenció que la administración del Área de Salud Cariari no dispone de indicadores de gestión que permitan efectuar una medición del desempeño de los funcionarios del Centro de Gestión Informática.

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. Ángel Ríos Maldonado, encargado de informática del Área de Salud Cariari manifestó[6]:

> *"(…) no se han definido indicadores de gestión, lo que se ha promovido son indicadores de producción desde la Dirección Regional. Los indicadores que se han definido son:*
>
> *- Número de incidencias atendidas en equipo TIC en Hardware y Software.*
> *- Número de trámites de compras.*
> *- Números de guías de reemplazo aplicadas.*
> *- Plan de contingencias en un periodo.*
> *- Parcheos o actualizaciones en Software.*
>
> *(…)*

A nivel local no se han establecido indicadores de la gestión de TI. Se entrega un informe anual que contiene la siguiente información:

- *Gestión Operativa.*
- *Soporte técnico*
- *Gestión Administrativa*

Y está compuesto de acciones, logros dificultades, alternativas de solución y observaciones."

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 esa área de salud en materia de tecnologías de información y comunicaciones.

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

2. GESTIÓN TÉCNICA DEL CENTRO DE GESTIÓN INFORMÁTICA

Se evidenciaron debilidades en la gestión operativa del Centro de Gestión Informática (CGI) del Área de Salud Cariari, 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, según se detalla seguidamente:

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

El Centro de Gestión Informática del Área de Salud Cariari carece de protocolos de seguridad para los activos informáticos, entre los que se encuentran computadoras, impresoras, redes y equipos de comunicación de datos, licencias y servidores, entre otros. Es importante señalar que, en la ubicación de los servidores de esa área de salud se pudo acceder a las licencias de los sistemas operativos de los mismos, sin restricciones y ubicada en un estante que no tiene medidas de seguridad.

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."*

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. Ángel Ríos Maldonado, coordinador del CGI, indicó que a nivel local no han elaborado protocolos que permitan establecer medidas de seguridad para los recursos informáticos; manifestó, además, que conocen a nivel de procesos lo que debe hacerse en cada caso pero que esa información no se ha documentado.

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 recursos que componen la infraestructura TIC de la unidad.

Se debe indicar que al momento de la evaluación los funcionarios de planta del CGI conocían y aplicaban correctamente las diversas herramientas de seguridad institucional; no obstante, como se indicó, la ausencia de protocolos que describan los procesos de implementación y cumplimiento de controles de seguridad, elevaría el nivel de riesgo de sufrir entre otros eventos 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 los funcionarios del Centro de Gestión Informática del Área de Salud Cariari no han sido capacitados en temas relacionados con sus funciones sustantivas, 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.

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 Manual citado 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, el citado manual indica lo siguiente:

> *"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. Ángel Ríos Maldonado, encargado del CGI en Área de Salud Cariari, indicó[7] lo siguiente:

"(…) no se cuenta con un plan de capacitaciones para los dos funcionarios del CGI, además no se tiene identificadas las necesidades en esta materia.

En el año 2016 se recibió capacitación institucional en materia de CCNA, redes de computadoras"

Respecto a la capacitación y asesoría a los usuarios el Ing. Ríos Maldonado indicó[8]:

"(…) *que se hicieron gestiones con la administración para ser incluidos en la capacitación del personal de nuevo ingreso para la divulgación de la normativa interna, no obstante, no se recibió respuesta."*

Las funciones definidas en el Modelo de Organización de los Centros de Gestión Informática representan una guía para el fortalecimiento del control interno, evaluación y fiscalización, con el fin de alcanzar los objetivos y metas establecidas por la organización en materia tecnológica.

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 del CGI 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.

Por lo anterior, 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.

El Centro de Gestión Informática del Área de Salud Cariari carece de un procedimiento formalmente establecido para la atención de solicitudes de soporte técnico, dado que atiende actualmente solicitudes generadas en el Sistema SOCO, así como las que se efectúan por medio de llamadas telefónicas, correos electrónicos o verbalmente.

[7] En entrevista escrita del 27 de marzo 2019.
[8] En entrevista escrita del 27 de marzo 2019.

Adicionalmente, al efectuar consulta en el SOCO sobre la cantidad de solicitudes atendidas desde el 1º de julio de 2018 al 22 de marzo de 2019, se contabilizan 122 casos, de forma tal que en promedio se atienden 13.5 mensualmente.

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. Ríos Maldonado, indicó[9]:

> "(…) *aproximadamente se atienden 200 incidencias, que corresponde a temas relacionados con conectividad de equipos, problemas de impresión, problemas de configuración de equipos, bloqueos de usuarios, cambios de contraseñas, acceso a sistemas, acceso a recursos compartidos, entre otros.*
>
> *No se tienen estadísticas de los tipos de incidentes que se atienden, ni de los usuarios que más requieren atención.*
>
> *(…) la diferencia corresponde a que el personal no utiliza la herramienta para hacer los reportes, lo hacen a través de correo electrónico, llamada telefónica y llegan a la puerta del CGI a solicitar la atención. En estos casos no se registra por parte del CGI la atención que se brinda".*

Ciertamente, la implementación de la herramienta denominada SOCO, que permite registrar las solicitudes de soporte técnico requerido por los funcionarios del área de salud es reciente, su utilización como medio institucional requiere un proceso de socialización y capacitación por parte de los usuarios involucrados en el proceso, que no ha sido efectuado por parte del Centro de Gestión Informática y la administración del área de salud.

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.

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

3. CONDICIONES DE SEGURIDAD FÍSICA Y AMBIENTALES DEL CENTRO DE GESTIÓN INFORMÁTICA DEL ÁREA DE SALUD CARIARI.

Se determinó que el Centro de Gestión Informática del Área de Salud Cariari tiene carencias en materia de seguridad física, entre las que destacan: ausencia de áreas separadas para ejecutar labores de mantenimiento, bodega de repuestos, suministros, archivos físicos; no existe una separación física del área dedicada a servidores, ni medidas de seguridad que impidan el acceso a estos equipos una vez se ingresa a la oficina del CGI. Además, se presenta acumulación de equipos, cables, repuestos, teclados y otros elementos ubicados en cajas.

Aunado a la anterior, existe una puerta interna que comunica la oficina de CGI con el archivo de expedientes del Ebáis Cariari 1, acceso que no dispone de medidas o mecanismos de control que limiten el ingreso al sitio.

Adicionalmente, se ubicaron equipos de cómputo nuevos y usados (monitores, UPS y otros) almacenados en el mencionado archivo de expedientes del Ebáis de Cariari 1, sin mecanismos de control de acceso.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo 1, punto 1.4.3 sobre seguridad física y ambiental indican lo siguiente:

> *"La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.*
>
> *Como parte de esa protección debe considerar:*
>
> *a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.*
> *b. La ubicación física segura de los recursos de TI.*
> *e. Los controles para el desecho y reutilización de recursos de TI.*
> *h. Los riesgos asociados con el ambiente"*

Las Políticas Institucionales de Seguridad Informática, en el apartado 10.13 refieren que:

> *"Todas las unidades de la CCSS deben velar porque el desecho del equipo de cómputo y componentes se realice periódicamente y con base en la normativa vigente, lo anterior con el fin de mantener los espacios físicos despejados".*

Las Normas de Control Interno para el Sector Público, emitidas por la Contraloría General de la República, señalan en su apartado 1 "Normas Generales", lo siguiente:

> *"El SCI de cada organización debe coadyuvar al cumplimiento de los siguientes objetivos:*

a. ***Proteger y conservar el patrimonio público contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*** *El SCI debe brindar a la organización una seguridad razonable de que su patrimonio se dedica al destino para el cual le fue suministrado, y de que se establezcan, apliquen y fortalezcan acciones específicas para prevenir su sustracción, desvío, desperdicio o menoscabo".*

Al respecto el Ing. Ríos Maldonado indicó[10] lo siguiente:

> *"(…) en el caso de acceso físico los servidores en uso en el área de salud no cuentan con seguridad, únicamente están alojadas en el CGI en un gabinete sin puertas. En acceso al CGI es restringido por medio de una puerta única de metal de la cual tiene llave la administración y los funcionarios del CGI.*
>
> *No obstante, una vez adentro se tiene acceso físico sin restricción a los servidores.*
>
> *En esos servidores se aloja información de bases de datos de SIIS, SIFA, Sistema de Vacunas, Reloj Marcador, Servidor de Archivos y Servidor DHCP y de Impresión. Que dan servicio a toda el área de salud.*
>
> *Además, el CGI tiene una puerta interna que comunica al archivo de expedientes activos de odontología y medicina general, la cual no cuenta con medidas de seguridad adecuadas para el acceso de terceras personas."*

Respecto a los activos ubicados en el archivo el Ing. Ríos Maldonado, indicó:

> "(…) *por disposición de la dirección se nos eliminó la bodega que se utilizaba para resguardo de archivos y activos y se tomó la decisión de almacenarlos en esa ubicación, el traslado fue efectuado por los trabajadores que efectuaron la remodelación. Esa condición se presenta desde el año 2016."*

Se debe indicar que la ocupación de espacios que originalmente no fueron diseñados para ser utilizados como Centros de Gestión Informática, así como para el almacenamiento de equipos tecnológicos o para la ubicación de servidores, unido a la inobservancia de la norma técnica relacionada con esta materia origina que no disponga de las condiciones adecuadas de resguardo de activos y ambientales para desarrollar las labores que le son asignadas institucionalmente.

La situación descrita expone los equipos informáticos ubicados en la oficina del CGI, a posibles daños, sustracciones o sabotaje de las personas que ingresen sin autorización en ese recinto o utilicen la puerta interna que comunica el archivo de expedientes del Ebáis Cariari 1 para ingresar en esa unidad. Además, se eleva el riesgo de afectar la continuidad de servicios que dependen de la información contenida en las bases de datos almacenados en los servidores que se custodian allí, comprometiendo el patrimonio institucional y la prestación de los servicios.

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

4. IMPLEMENTACIÓN DEL EXPEDIENTE DIGITAL ÚNICO EN SALUD EN EL SERVICIO DE URGENCIAS Y LOS PUESTOS DE VISITA PERIÓDICA

Se evidenció que el Expediente Digital Único en Salud se ha implementado parcialmente en el Servicio de Urgencias y en los Puestos de Visita Periódica del Área de Salud Cariari. En ambos casos se incluye la información en el Sistema de Identificación, Agendas y Citas (SIAC), no obstante, no se registran los datos relacionados con la valoración de enfermería y la atención médica.

En el Servicio de Urgencias el flujo de datos se inicia con la apertura de la atención por parte de los funcionarios de REDES, en donde se incluye la información del asegurado en el SIAC y se imprime la hoja de atención, posteriormente el usuario recibe la valoración médica[11] y se realizan las anotaciones a mano en la hoja impresa. Finalmente, la atención es cerrada en el SIAC por el Servicio de REDES incluyendo en el sistema únicamente el diagnóstico.

En los puestos de visita periódica, se procede a ingresar en el SIAC la agenda de citas previamente elaborada por el comité local de salud, información con la cual se procede a la preconsulta de enfermería y consulta del médico.

Posteriormente la funcionaria de REDES cierra la consulta en el SIAC, incluyendo los diagnósticos correspondientes.

Al finalizar estas consultas no se dispone de la información de los asegurados relacionada con: procedimientos de enfermería, valoración médica, anotaciones de observación de pacientes, referencias, entre otros.

La Ley del Expediente Digital Único en Salud Nº 9162 del mes de agosto del 2013, articulo 1, 3 y en el transitorio único, señala:

> *"ARTÍCULO 1.- Finalidad*
>
> *Se entiende por expediente digital único de salud el repositorio de los datos del paciente en formato digital, que se almacenan e intercambian de manera segura y puede ser accedido por múltiples usuarios autorizados. Contiene información retrospectiva, concurrente y prospectiva, y su principal propósito es soportar de manera continua, eficiente, con calidad e integralidad la atención de cuidados de salud."*
> *(…)*

[11] Incluye valoración general del estado del paciente y plan a seguir.

ARTÍCULO 3.- Objetivos de esta ley

Son objetivos de esta ley:

a) Fortalecer la garantía constitucional del derecho a la vida y a la salud de los habitantes de la República, por medio del desarrollo y la creación del expediente digital único de salud en beneficio de todas las personas, incrementando la calidad de los servicios de salud que recibe la población.

b) Avanzar hacia la universalidad en el acceso a los servicios médicos de calidad, bajo una integración funcional de las instituciones públicas del sector salud.

c) Que cada persona tenga un expediente electrónico con la información de toda la historia de atención médica, con las características de disponibilidad, integridad y confidencialidad.

d) Reducir la brecha de equidad existente en la prestación de servicios de salud en las diversas regiones del país.

e) Promover la interoperabilidad de la información, el procesamiento, la confidencialidad, la seguridad y el uso de estándares y protocolos entre las distintas entidades del sector salud, de forma tal que se tenga acceso seguro y oportuno a la información de las personas que requieren atención, conforme a los principios del consentimiento informado y la autodeterminación informativa.
(…)
TRANSITORIO ÚNICO. -

La Caja Costarricense de Seguro Social tendrá cinco años, a partir de la vigencia de la presente ley, para asegurar el cumplimiento en todo el territorio nacional de los objetivos dispuestos por esta ley. Se entenderá que hasta los primeros tres años de ese quinquenio serán para la implementación en el primer nivel de atención y que al final de los cinco años deberá estar implementado el expediente digital único de salud en el nivel hospitalario."

Sobre la implementación parcial del EDUS[12] en el servicio de Urgencias el Ing. Ángel Ríos Maldonado, refirió[13] lo siguiente:

"(…) se tiene un edificio muy antiguo en el cual en su construcción no se consideró la necesidad de dotarlo de red datos, además de que cuenta con una red eléctrica que no asegura el buen funcionamiento de todos los equipos necesarios, tampoco tiene la disponibilidad de conectar nuevos dispositivos.

[12] Expediente Digital Único en Salud.
[13] En entrevista escrita del 27 de marzo 2019.

Con base en lo anterior, en el año 2014, nos visitó el equipo implementador del proyecto EDUS ellos acordaron implementar EDUS-Urgencias como uno de los primeros del país, se analizaron las necesidades en el sitio, de esto no hubo resultados.

En el 2015 el enfoque de EDUS fue cambiar conexiones de cobre por fibra óptica, por lo que no se consideró incluir urgencias al estar en funcionamiento el SIAC, aún no estaba el SIIS.

En el 2016 El proyecto EDUS brinda equipos en la modalidad Leasing, para los centros que contaban con conexiones de fibra, tampoco se consideró la inclusión de urgencias, además de parte nuestra enviamos oficio para recordar el acuerdo de implementación del EDUS en urgencias, de esta gestión no obtuvimos respuestas.

En el 2017 se desarrolla la obra interna en los EBÁIS y tampoco se consideró la implementación en urgencia, en ese mismo año se solicita al EDUS la implementación en ese servicio acompañado de farmacia, trabajo social., psicología, laboratorio clínico y odontología.

Ese mismo año había una propuesta llamada "Proyecto Sabana" entre la Dirección Regional y la DTIC para solventar las necesidades de equipo para el proyecto EDUS, en nuestro caso lo que se hizo fue consultarle al director de proyecto EDUS si ese proyecto estaba asociado a ellos a lo que el Ing. Roberto Blanco, director de implementación respondió que el desconocía el proyecto y que no estaban trabajando en conjunto. Por lo que se tomó la decisión de no invertir y esperar que el proyecto EDUS diera los equipos y solucionara las necesidades eléctricas y de red de datos.

Durante el año 2018, EDUS propone entregarnos equipos activos, pero sin la red eléctrica y de datos, la Dirección rechazó esta propuesta pues persisten las condiciones de ausencia de red de datos e insuficiencia en la red eléctrica.

El 15 de enero del 2019 solicitamos una visita del director del proyecto para la valoración y se acordó que se implementara en el primer semestre.

A la fecha no se han iniciado las obras necesarias para la implementación."

En relación con la implementación en los puestos de visita periódica, el Ing. Ríos Maldonado, señaló[14]:

"(…) actualmente los PVP que son visitados por el Ebáis móvil no cuentan con conexión a EDUS dado que están ubicados en comunidades que no cuentan con acceso a redes de datos o de celular.

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

(…) en el año 2018 se procedió a utilizar un dispositivo de conexión móvil (MIFI) para poder probar la calidad de la conexión en todos los puestos de visita periodo, los resultados fueron negativos en todos, al no tener señal celular, por esa situación no se ha implementado en los puestos de visita. A pesar de esa situación en el proyecto FONATEL de fortaleciendo del EDUS se cuenta con Tablets equipadas para que sean utilizadas."

Las condiciones de planta física del Servicio de Urgencias del Área de Salud Cariari relacionadas con la dotación de red eléctrica y de datos no han permitido la habilitación del todos los componentes del Expediente Digital Único en Salud, lo anterior, a pesar de múltiples gestiones que se han hecho desde la Dirección del Área con el equipo implementador de la Dirección de Tecnologías.

Adicionalmente, en los puestos de visita periódica se han detectado serias dificultades de acceso a la red móvil, lo que ha provocado que a la fecha no sea factible la interacción con el expediente de los funcionarios que se desplazan a esos puestos.

La situación descrita permite que se cierre una atención médica sin completar la información correspondiente en el Expediente Digital Único en Salud, de los pacientes que son atendidos por el Servicio de Urgencias en el Área de Salud y en los puestos de visita periódica, entre los datos relevantes que no se están incluyendo se tiene valoración de enfermería, procedimientos de enfermería, valoración del médico, planes de acción entre otros, provocando que en caso de ser atendido por otra unidad o servicio no sean accesibles dichos datos y perdiendo la trazabilidad y confiabilidad de la información del asegurado.

Es importante indicar que por la ubicación geográfica del Área de Salud Cariari, la información relevante que no está siendo registrada en el EDUS corresponde a poblaciones de alta vulnerabilidad, dado que se ubican en zonas rurales y de niveles de pobreza elevados, comprometiendo el principio de igualdad que rige las acciones institucionales.

CONCLUSIÓN

La gestión en 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 Centro de Gestión Informática (CGI) del Área de Salud Cariari, se evidenciaron debilidades en la definición de los procesos sustantivos que ejecuta, identificación de los riesgos incluidos en Plan de Continuidad de la Gestión, en la elaboración del Plan Anual Operativo y su seguimiento e indicadores de gestión. Adicionalmente en la gestión operativa en lo relacionado con el desarrollo e implementación de protocolos de seguridad para el aseguramiento de los activos informáticos, elaboración y desarrollo de planes de capacitación y registro de atención de incidencias.

En lo referente a las condiciones de seguridad física, es necesario indicar que el carecer de mecanismos de control de acceso a los servidores, así como la posibilidad de acceder por la puerta interna, se constituyen en elementos que elevan el riesgo de sustracciones, intrusiones no autorizadas o sabotaje sobre todos los elementos que se resguardan en esa oficina, esta situación es incluso más elevada para los equipos (monitores nuevos y usados, ups usadas y otros) que son almacenados en el archivo de expedientes del Ebáis Cariari 1, los cuales no disponen de medidas de seguridad.

Finalmente, la implementación parcial del EDUS en el servicio de Urgencias y en los Puestos de Visita Periódica, expone a los asegurados al registro incompleto de la información que se genera en cada atención que reciben en esos puntos. Esta condición compromete datos relevantes de población vulnerable ubicada en sectores rurales, de difícil acceso y en la mayoría de los casos de un nivel elevado de pobreza, los que tendrían una información parcial en caso de ser atendidos en otra unidad institucional.

La condición descrita, además, dificultaría la toma de decisiones relacionadas con esa población en aspectos de la planificación de los servicios de salud, al tener solamente el registro con el diagnóstico de cada atención.

RECOMENDACIONES

AL ING. MANUEL RODRÍGUEZ ARCE, DIRECTOR DEL PROYECTO EXPEDIENTE DIGITAL ÚNICO EN SALUD, O QUIEN EN SU LUGAR OCUPE EL CARGO

1. Diseñar e implementar un plan de acción que garantice la inclusión en el Expediente Digital Único en Salud de la información que se genera en una consulta del Servicio de Urgencias y de los puestos de visita periódica del Área de Salud Cariari (hallazgo 4).

Para acreditar el cumplimiento de la recomendación se deberá remitir a esta Auditoría la documentación que respalde la implementación de las soluciones determinadas en el plan, en un plazo de 9 meses a partir del recibo del informe.

AL LIC. JORGE ANTONIO OVIEDO PRADO, ADMINISTRADOR DEL ÁREA DE SALUD CARIARI, O QUIEN EN SU LUGAR OCUPE EL CARGO.

2. Definir y documentar en coordinación con el encargado del CGI los procesos relevantes que deben ser atendidos por el Centro de Gestión Informática, conforme a lo indicado en el apartado 1.1 de este informe.

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 relevantes, debidamente aprobados por parte de esa Administración.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

3. Garantizar en conjunto con el encargado de Gestión Informática la ejecución de las siguientes acciones relacionadas con el Plan de Continuidad (hallazgo1.2):

a. Incluir riesgos que respondan a un análisis de las vulnerabilidades de la zona donde se ubica la sede del área, así como de sus Ebáis.
b. Analizar el nivel de criticidad de los equipos de TIC con la finalidad de incluir aquellos que se consideren críticos para la prestación de los servicios, en su defecto de sustentar que no existen equipos con ese nivel en el Área de Salud.
c. Ajustar las acciones a ejecutar durante y después de que ocurra un evento para cada uno de los riesgos incluidos en el Plan de Continuidad.

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 vulnerabilidades y riesgos a incluir en el Plan de Continuidad (inciso a), el análisis de nivel de criticidad de los equipos TIC (inciso b) y las acciones a ejecutar que correspondan a cada uno de los riesgos que se incluyan en el Plan (inciso c).

4. Definir en conjunto con 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 (hallazgo 1.3).

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.

5. Definir los indicadores de gestión necesarios para evaluar el cumplimiento de las labores sustantivas que deben ejecutar los funcionarios del Centro de Gestión Informática e implementar los mecanismos necesarios de control para asegurar la supervisión y análisis del comportamiento de dichos indicadores (hallazgo 1.4).

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, mecanismos de control y supervisión definidos del personal establecidos.

6. Implementar en coordinación con el encargado de gestión TIC los protocolos de seguridad para los activos informáticos disponibles en esa área de salud.

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 (hallazgo 2.1).

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

7. Elaborar un plan de capacitación dirigido a fortalecer los conocimientos y capacidades de los funcionarios en tecnologías de información del área de salud, 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 (hallazgo 2.2).

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.

8. Establecer un procedimiento para la atención de solicitudes de soporte técnico, las cuales deberán ser registradas en el SOCO, herramienta institucional diseñada para el control y registro de actividades (hallazgo 2.3).

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.

9. Efectuar un análisis de los espacios disponibles con el fin de establecer un plan de abordaje que permita fortalecer las condiciones de seguridad física del Centro de Gestión Informática, considerando entre otros los siguientes aspectos (hallazgo 3):

a. Separación física del área dedicada a los servidores.
b. Restricción de acceso al archivo de expedientes del Ebáis Cariari 1.
c. Reubicación de los activos almacenados en el archivo de expedientes del Ebáis Cariari 1.
d. Establecimiento de un área dedicada a soporte técnico y revisión de equipos.
e. Reubicación en un área de almacenaje de todos los elementos ubicados en cajas (teclados, cables, otros) en el espacio del CGI.

Para acreditar el cumplimiento de la recomendación deberá aportarse evidencia del análisis solicitado y el plan de abordaje con responsables y fechas de implementación.

Plazo de cumplimiento: 9 meses a partir del recibo de este 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 Ing. Manuel Rodriguez Arce, Director, Licda. Xinia Cordero Sobalbarro, Jefe de Implementación de aplicaciones, ambos funcionarios del Proyecto Expediente Digital Único en Salud, quienes no hacen comentarios y aceptan los alcances de la recomendación 1.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax: 2539-0888
Apdo. 10105

Además, se comentó con el Dr. Henrick Miles Ramsey, Director, Licda. Leidy Solano Castro, Administradora a.i, Ing. Fredy Alvarez Varela, encargado de TI a.i, todos del Área de Salud Cariari. La Licda. Solano Castro solicitó ampliar el plazo de cumplimiento de la recomendación número 9, a 9 meses, dado que se deberán hacer ajustes correspondientes a infraestructura física.

El cambio solicitado fue valorado y aceptado por esta Auditoría, el mismo se incluye en el presente informe.

ÁREA GESTIÓN OPERATIVA

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

Br. Alexander Araya Mora
ASISTENTE DE AUDITORÍA

ORIANA MATARRITA HERNANDEZ (FIRMA)
Firmado digitalmente por ORIANA MATARRITA HERNANDEZ (FIRMA)
Fecha: 2019.06.17 11:39:42 -06'00'

Licda. Oriana Matarrita Hernández
ASISTENTE DE AUDITORÍA

MIGUEL ANGEL SALVATIERRA ROJAS (FIRMA)
Firmado digitalmente por MIGUEL ANGEL SALVATIERRA ROJAS (FIRMA)
Fecha: 2019.06.21 14:10:43 -06'00'

Ing. Miguel Ángel Salvatierra Rojas
JEFE DE SUBÁREA

MASR/AAM/OMH/edvz