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

AGO-34-2018
27-4-2018

RESUMEN EJECUTIVO

El estudio se realizó de conformidad con el Plan Anual de Trabajo 2018 del Área Gestión Operativa, apartado actividades programadas, con el propósito evaluar la gestión del Centro de Gestión Informática del Área del Centro de Atención Integral en Salud de Siquirres.

Los resultados del presente informe evidencian debilidades respecto a la identificación de los procesos sustantivos que ejecuta el CGI, así como en la definición, valoración y actualización de los riesgos que podría enfrentar la plataforma de tecnologías de información y comunicaciones que presta servicio en esa unidad. Adicionalmente, no se han implementado las observaciones emitidas por la Sub Área de Continuidad relacionadas con la documentación de los controles existentes para la mitigación, así como con la actualización de la metodología de valoración y la actualización del mapa de riesgos.

En relación con el Plan Anual, se incluyen objetivos que representan actividades propias de la gestión administrativa y técnica como la actualización de documentos, entre los que destaca el Plan de Continuidad, Estudios de Necesidades, Inventarios de Equipos, entre otros, siendo estos insumos para el establecimiento de una planificación basada en metas que permitan un desarrollo ordenado de las TIC en esa Área. En el desarrollo del estudio, se determinaron diferencias en el inventario de componentes y dispositivos utilizados para mantenimiento correctivo respecto de lo reportado en la base de datos del sistema SOS.

En virtud de los resultados se emiten 7 recomendaciones dirigidas a las autoridades del CAIS de Siquirres, con la finalidad de fortalecer los procesos de planificación anual, medición de la gestión y productividad del CGI, definición y atención de riesgos, capacitación del personal y control de inventario de stock de componentes.

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

AGO-34-2018
27-4-2018

ÁREA GESTIÓN OPERATIVA
AUDITORÍA DE CARÁCTER ESPECIAL SOBRE EVALUACIÓN INTEGRAL EN EL ÁREA DE SALUD DE SIQUIRRES U.E 2631.
TEMA: GESTIÓN CENTRO DE GESTIÓN INFORMÁTICA.

ORIGEN

El presente estudio se realizó en atención al Plan Anual Operativo del Área Gestión Operativa para el año 2018.

OBJETIVO GENERAL

Evaluar la gestión del Centro de Gestión Informática del Área del Centro de Atención Integral en Salud de Siquirres.

OBJETIVOS ESPECÍFICOS

- Determinar el cumplimiento de las funciones sustantivas del Centro de Gestión Informática del Área de Salud, su debida documentación, asignación de responsables y apego a la planificación estratégica de la institución.

- Evaluar la suficiencia y oportunidad de la gestión y planificación del Centro de Gestión Informática del Área de Salud, en aspectos como planificación de actividades, gestión de riegos, administración de proyectos, mantenimiento y reparación de equipos.

- Determinar aspectos relevantes de la Estructura Organizacional y Funcional, Plataforma Tecnológica (Hardware, Software y Telecomunicaciones) y Gestión de Recursos Financieros del Centro de Gestión Informática del Área de Salud, de manera que respondan a las necesidades actuales de dicho Centro de Salud y se ajustan a las políticas institucionales.

- Comprobar la efectiva aplicación de la Normativa Técnica y Jurídica aplicable en los procesos de trabajo que realiza el Centro de Gestión Informática del Área de Salud, en cumplimiento con el marco jurídico aplicable.

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

ALCANCE

El estudio comprende la revisión y análisis de las actividades sustantivas propias del Centro de Gestión Informática del Área de Salud durante los años 2016-2017, ampliándose en aquellos casos que se considere 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 2016-2017.
- Análisis del Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones.
- Análisis de la Autoevaluación de Riesgos del CAIS de Siquirres.
- Inventario en bodega de stock de dispositivos y componentes.
- Entrevista a Msc. Deiler Calvo Matamoros, Coordinador del Centro de Gestión Informática CAIS Siquirres.

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.

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

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:

> *"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. **Sobre la definición de los procesos que ejecuta el Centro de Gestión Informática.**

Se evidenció que el Centro de Gestión Informática del Centro de Atención Integral en Salud (CAIS) de Siquirres no ha definido de manera formal los procesos que debe ejecutar en atención a sus funciones.

Al respecto, se verificó que a partir del 2015 se estableció un esquema de responsabilidades para cada uno de los perfiles ocupacionales con que se dispone, el cual al momento de la evaluación no ha sido revisado y en caso de considerarse necesario, actualizado.

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*".

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

El Msc. Deiler Calvo Matamoros, encargado del CGI[1] del CAIS de Siquirres, manifestó [2] que:

"La determinación de procesos relevantes para el CGI local se ha efectuado acorde al Modelo de Organización de CGIs aprovechando al máximo las capacidades del recurso humano actualmente disponible en planta conforme al perfil del cargo que ocupan, atendiendo temas de gestión técnica y soporte administrativo."

Añadió, además:

"Bajo este escenario desempeñamos actividades como las que a continuación se mencionan:

1. Administrar proyectos relacionados con TIC.
2. Elaborar estudios técnicos y preliminares para adquisición de bienes o servicios.
3. Proveer confiabilidad y oportunidad de la información.
4. Administrar el servicio de telefonía IP y recurso pasivo y activo de comunicaciones.
5. Implementar actividades orientadas a la seguridad informática.
6. Gestionar la adquisición de software y hardware de acuerdo con necesidades de la organización.
7. Gestionar capacitación técnica.
8. Brindar soporte a programas de telesalud, videoconferencias y procesos de formación en línea.
9. Velar por el cumplimiento de las políticas, normas y estándares en materia de TIC dictadas en el marco institucional.
10. Gestionar el tratamiento de desechos relacionados con el área de nuestra competencia.
11. Capacitar y asesor a usuarios de la plataforma tecnológica.
12. Administrar bases de datos.
13. Elaborar/actualizar planes de continuidad del negocio.
14. Instalar aplicaciones, brindar soporte técnico y control de licencias y/o recursos institucionales.
15. Mantenimiento de la plataforma de TIC.
16. Dirigir, coordinar, supervisar y evaluar las actividades sustantivas.
17. Controlar el uso eficiente y eficaz del recurso humano, físico, tecnológico y material asignado y en toda la Unidad.
18. Participar en el proceso de elaboración del plan operativo y presupuesto del CAIS."

Ciertamente el CGI ha establecido de conformidad con los perfiles de recursos humanos que dispone, las acciones que debe ejecutar en sus labores diarias, no obstante, no ha considerado la identificación de sus procesos relevantes y que se encuentran claramente establecidos en el Manual de Organización correspondiente.

[1] Centro de Gestión Informática
[2] Entrevista escrita, 5 de marzo 2018

Es necesario indicar que la ausencia de identificación de los procesos responsabilidad del CGI, puede ocasionar que los esfuerzos en la atención diaria de requerimientos y solicitudes de soporte técnico, así como en las acciones operativas propias, impida la atención de otras responsabilidades relevantes, tales como desarrollo de cultura organizacional, participación en la regulación y normativa técnica, simplificación de trámites, entre otros, provocando eventuales afectaciones en la prestación de los servicios de tecnologías de información y comunicaciones, lo que finalmente representaría un impacto para la atención de los usuarios, en las actividades que requieren el apoyo de estas tecnologías.

2. Sobre la identificación de Riesgos en Tecnologías de Información.

Se evidenció la ausencia de revisión periódica de los riesgos y su debida actualización; además, el CGI no ha identificado riesgos propios de las funciones que desempeña el departamento.

El Centro de Gestión Informática ha definido para el CAIS de Siquirres los siguientes riesgos relacionados con tecnologías de información y comunicaciones: averías en servidores, fallo en comunicaciones, falla en equipos críticos de comunicación, perdida de información crítica, averías en PC y/o impresoras, violaciones a la seguridad física, virus, interrupciones eléctricas y desastres naturales, además, se han establecido acciones de mitigación, responsables y resultados esperados para cada riesgo.

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."

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.

(…)

[3] 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."

El Msc. Deiler Calvo Matamoros, encargado del CGI del CAIS de Siquirres, manifestó lo siguiente con respecto [4] al proceso utilizado para definir los riesgos:

"Apoyados en los recursos distribuidos por la DTIC en materia de gestión de riesgos desde el CGI se determinan peligros naturales o provocados (internos y externos) a los que se encuentra expuesta la Unidad cuya materialización impactaría la plataforma tecnológica de manera negativa.

El ejercicio se efectúa considerando categorías de riesgos como interrupción eléctrica, fallos en hardware, fallos en comunicaciones (recurso activo y pasivo), desastre natural, fallos en respaldos, virus, violaciones a la seguridad física y recurso humano."

Respecto a la revisión y actualización de los riesgos, el Msc. Calvo Matamoros indicó[5]:

"El CGI de manera periódica evalúa los peligros y las acciones realizadas en la ejecución de controles de mitigación para los riesgos determinados en un tiempo en específico."

Lo descrito, muestra la ausencia de mecanismos o procedimientos que permitan llevar a cabo revisiones periódicas de los riesgos establecidos para la plataforma de tecnologías de información y comunicaciones del CAIS Siquirres, aun cuando se ejecutó el traslado a las nuevas instalaciones ubicadas en las afueras de la localidad y que presenta condiciones externas e internas que difieren de su ubicación anterior.

La identificación adecuada de los riesgos, determina los eventos o situaciones que puedan afectar adversamente la prestación de los servicios a nivel institucional y/o local, evaluando los posibles daños así como las acciones requeridas para prevenir o minimizar los efectos de una pérdida parcial o total, además, el análisis de riesgos y su evaluación y actualización constante permite fortalecer el desarrollo de la planificación estratégica del Área y del CGI, de forma tal que su actualización y revisión constante permite minimizar el eventual impacto que enfrentaría la unidad en la continuidad de sus servicios.

3. Sobre la implementación y cumplimiento de controles de seguridad y emergencia con respecto al aseguramiento de los recursos informáticos.

El Centro de Gestión Informática del CAIS de Siquirres, no ha elaborado protocolos para la implementación de controles de seguridad de los recursos informáticos, no obstante, se evidencia la aplicación de medidas de carácter institucional a efectos de brindar protección a esos activos, entre los más relevantes destacan:

[4] Entrevista escrita, 1º de marzo 2018.
[5] Entrevista escrita, 1º de marzo 2018.

- Politica seguridad informática TIC institucional.
- Mejores prácticas en centro de procesamiento datos.
- Configuración segura equipos.
- Procedimiento mal uso internet.
- Procedimiento revisión equipo computo.
- Guía elaboración respaldos.
- Guía de buenas prácticas TIC.
- Lista oficial software.
- Capacitación usuarios finales.
- Clausulas confidencialidad información contratos por terceros.
- Monitoreo CMC.
- Comunicados seguridad informática (correos 2017 | plan remedial | seguridad informática).
- Desechos informáticos.
- Confidencialidad de la información.
- Navegación internet (perfiles otorgados usuarios finales).

Adicionalmente, se cuenta con accesos restringidos y con llave tanto a cuartos de comunicaciones como de servidores y a la bodega de stock de repuestos.

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 Msc. Deiler Calvo Matamoros, encargado del CGI del CAIS de Siquirres, manifestó[6] que:

"*Respecto al tema de seguridad en tecnologías de información el CGI local aplica la normativa institucional que a continuación se detalla:*

- *Políticas institucionales de seguridad informática, TIC-Seguridad-001.*
- *Normas institucionales de seguridad informática, TIC-ASC-SEG-002.*
- *Guía de mejores prácticas en la gestión de los centros de producción de datos, DTI-SI-003.*
- *Guía para la configuración segura de equipos, TIC-SEG-004, considerando la lista oficial de software libre o gratuito autorizado en la CCSS, DTI-I-SI-0016, v 1.5.0.*
- *Procedimiento mal uso del servicio de internet en la CCSS, TIC-ASC-SEG-005.*
- *Guía para la elaboración de respaldos, DTI-I-CP-0020.*
- *Guía usuario final buenas prácticas en uso de las TIC, DTI-I-SI-0010.*

[6] Mediante cedula narrativa del 1 de marzo 2018.

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

A partir de la normativa institucional detallada los procedimientos efectuados son los siguientes:

1. *Control acceso a recursos institucionales.*

   Este tema es atendido desde dos escenarios. El primero a partir del control de acceso a la información/aplicaciones y el segundo a partir del control de acceso a la infraestructura técnica, para ambos casos el CGI local vela y garantiza que cada funcionario únicamente tenga acceso a la información y recursos estrictamente necesarios para el desarrollo de su función por medio de:

   1.1 Que cada colaborador de la Unidad cuente y utilice usuario institucional propio.

   Actualmente se aplica el procedimiento de gestión de cuentas de usuarios de red institucional, oficio No. 7391 suscrito por el Doctor Wilman Rojas Molina, Director Regional, DRSSHA, para creación, eliminación, bloqueo, modificación u otras actividades relacionadas con de cuentas de usuario institucional.

   1.2 Transferencia de conocimiento, promoción y capacitación continua en materia de seguridad informática y uso adecuado de recursos TIC (correo electrónico institucional, equipos de trabajo, red de datos, unidades de respaldo externas, otros).

   1.3 Acceso exclusivo del personal de CGI al directorio activo. Periódicamente se contribuye con la actualización de este recurso.

   1.4 Aplicación de la configuración segura de equipos dictada por la institución.

   1.5 Administrar por parte del CGI, cuentas y contraseñas de administrador de estaciones de trabajo, servidores y equipo activo de comunicaciones.

   1.6 Existencia de administradores locales para MISE para aplicativos EDUS.

   1.7 Mantenimiento y actualización continua de aplicaciones y parcheo de equipos.

   1.8 Aplicar cláusulas de confidencialidad de la información institucional y trato con terceros.

   1.9 Se cuenta con cuartos y entornos exclusivos para resguardar el equipo activo de comunicación y centro de datos con particularidades desarrolladas que giran alrededor de la guía de mejores prácticas en la gestión de los centros de producción de datos. Para este punto destaca que desde el CGI se ha promovido la implementación de sistemas/medios electrónicos para control de acceso.

1.10 Monitoreo periódico de Configuration Manager Console (CMC) y cuartos de producción y centro de datos.

1.11 Instaladores y licencias institucionales, recursos administrados exclusivamente por personal del CGI.

2. Respaldos de información.

Este punto particularmente se relaciona con el respaldo de la información crítica de la Unidad generada por sistemas, bases de datos e información de puestos de trabajo clave para la organización. Bajo este escenario y la normativa institucional en este tema localmente se aplica lo que a continuación se detalla:

2.1 Metodología local de respaldos apoyados en la guía para elaboración de respaldos institucional.

2.2 Monitoreo periódico de la metodología de respaldos implementada para verificar su efectiva ejecución.

3. Aseguramiento de recursos informáticos.

Dentro de este tema se ejecuta lo que a continuación se menciona:

3.1 Contar con Centro de Operaciones de Emergencia (COE), actualmente implementado, equipado e identificado en la antigua sede de área.

3.2 Elaboración/actualización del Plan de Continuidad en TIC (PCTIC).

3.3 Ejecución de ensayos de restauración de servicios/sistemas de alta criticidad.

3.4 Almacenamiento de respaldos en sitio alterno a la fuente original de información.

3.5 Mantener en la medida de las posibilidades, vigentes contratos de mantenimiento preventivo y correctivo de la plataforma tecnológica."

Todo lo anterior conforme las políticas, normas, guías y procedimientos establecidos por la institución para aplicación general (per se de aplicación obligatoria), así las cosas a la fecha a excepción del PTIC, no se han gestionado protocolos de seguridad informática aprobados por la jefatura administrativa."

El CGI de Siquirres ha adoptado los mecanismos institucionales relacionados con la seguridad de los recursos informáticos, no obstante, a nivel local no se ha establecido la necesidad de gestionar protocolos propios a efectos de reflejar las condiciones que se presentan en la zona.

La situación descrita favorecería el debilitamiento de las acciones relacionadas con la protección de los diversos recursos informáticos, ante la ausencia de los funcionarios que ya conocen la aplicación de las diferentes políticas institucionales elevando el nivel de exposición al riesgo de la plataforma tecnológica del CAIS.

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, aunado a una posible ausencia de esos funcionarios debilitaría la aplicación de los controles establecidos y elevaría su nivel de riesgo.

4. Sobre la atención de las observaciones emitidas por la Sub Área de Continuidad relacionadas con el Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones

Se evidenció la elaboración del Plan de Contingencia de Tecnologías de Información y Comunicaciones por parte del Centro de Gestión Informática del CAIS-Área de Salud de Siquirres, no obstante, no se han realizado acciones a efectos de implementar las observaciones emitidas por la Sub Área de Continuidad de la Dirección de Tecnologías[7] relacionadas con la documentación de los controles existentes para la mitigación de los riesgos, actualización de la metodología de valoración de riesgos y del mapa de riesgos.

Además, no se evidencia la ejecución de la totalidad de los ensayos que se planifican, así como la inclusión de los resultados del ensayo ejecutado en el año 2017.

El Manual para elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones de la DTIC[8], 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."

[7] Documento SCGTIC-039-2016 "Informe sobre la evaluación del Plan de Continuidad de la Gestión TIC Área de Salud de Siquirres, E.U 2631"
[8] Dirección de Tecnologías de Información y Comunicaciones

El Msc. Deiler Calvo Matamoros, encargado del CGI del CAIS de Siquirres, manifestó respecto al proceso de utilizado para definir los riesgos, lo siguiente[9]:

"Apoyados en los recursos distribuidos por la DTIC en materia de gestión de riesgos desde el CGI se determinan peligros naturales o provocados (internos y externos) a los que se encuentra expuesta la Unidad cuya materialización impactaría la plataforma tecnológica de manera negativa.

El ejercicio se efectúa considerando categorías de riesgos como interrupción eléctrica, fallos en hardware, fallos en comunicaciones (recurso activo y pasivo), desastre natural, fallos en respaldos, virus, violaciones a la seguridad física y recurso humano."

Respecto a la revisión y actualización de los riesgos, el Msc. Calvo Matamoros indicó:

"El CGI de manera periódica evalúa los peligros y las acciones realizadas en la ejecución de controles de mitigación para los riesgos determinados en un tiempo en específico."

Además, indicó que no se han efectuado los ensayos debido a la alta demanda de servicios por parte de los usuarios de la plataforma y la atención de otras responsabilidades[10].

La constante demanda de soporte técnico por parte de los usuarios del CAIS, la ejecución de labores administrativas, así como de la ausencia de definición de los procesos relevantes para el CGI según se indicó en el hallazgo 1 del presente informe, podría ocasionar que no se atiendan las observaciones emitidas por la Sub Área de Continuidad y se incumpla con los ensayos programados en el año.

El fin último de la infraestructura tecnología es la prestación de servicios a los asegurados, situación que estaría comprometida ante la falta de oportunidad en la atención de eventos que comprometan su estabilidad y continuidad, aunado a lo anterior se pone en eventual riesgo equipos, sistemas y componentes de red de alto valor económico.

5. Sobre la Planificación Anual del Centro de Gestión Informática.

El Centro de Gestión Informática del CAIS de Siquirres elabora el documento denominado "Plan 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, dicha planificación presenta los siguientes aspectos sujetos de mejora:

- **Inclusión de objetivos y actividades que corresponden a responsabilidades propias del CGI**

En el "Plan Operativo" del CGI se incluye para los años 2016 y 2017 objetivos que corresponden a las actividades propias de la gestión tales como: Actualizar el inventario de hardware y software de Tecnologías de Información y Comunicaciones (TIC), Actualizar el Estudio de Necesidades de TIC,

[9] Entrevista escrita, 1º de marzo 2018.
10 Entrevista escrita, 1º de marzo 2018.

Actualizar el Plan de Continuidad de Tecnologías de Información y Comunicaciones (PCTIC), Evaluar el nivel de reemplazo de activos de TIC, siendo que estos documentos deberían considerarse como insumos para establecer metas de desarrollo y crecimiento de los servicios.

- **Carencia de indicadores avance y cumplimiento de las metas**

El "Plan Operativo" del CGI carece de indicadores que permitan conocer el avance real en el cumplimiento de las metas establecidas, dado que solamente indica los productos que se entregaran en cada semestre, dificultando conocer el nivel de cumplimiento.

- **Incumplimiento de las metas establecidas**

Se evidenció el incumplimiento de metas programadas tales como:

- Actualización del Plan de Continuidad, como se indicó en el hallazgo 4 del presente informe, el PCTIC[11], no fue actualizado en el año 2017, además, se programaron 4 ensayos (2 en cada periodo) de los cuales únicamente se realizaron el 50%.

  Adicionalmente, no se han atendido las recomendaciones de la DTIC, respecto a actualizar la definición y valoración de los riesgos.

- Elaboración mensual de informes de producción, se programó la elaboración de 12 informes para cada periodo, no obstante, solamente fueron evidenciados 19 informes enviados a la administración del CAIS.

- Ofrecer un sitio colaborativo que facilite la gestión operativa departamental, se realizaron las solicitudes a nivel de la Dirección Regional de Servicios de Salud para contar con el sitio colaborativo, sin embargo, no ha sido habilitado.

- Efectuar las acciones necesarias para dotación de (1) profesional y (2) técnicos en TIC, solamente se incluyó como un apartado en el documento denominado "Estudio de Necesidades 2017", no obstante, no se evidenciaron acciones relacionadas con el proceso de solicitud de los recursos necesarios para atender esta necesidad.

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,*

[11] Plan de Continuidad de Tecnologías de Información y Comunicaciones.

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."

El Msc. Deiler Calvo Matamoros, encargado del CGI del CAIS de Siquirres, al respecto manifestó[12]:

"Los indicadores integrados en el Plan Operativo anual permite medir el avance de cumplimiento de objetivos y metas planteados para el periodo."

La inclusión de actividades relacionadas con la gestión documental del CGI como metas de la planificación anual, podría ocasionar la falta de oportunidad en la atención de otras áreas que eventualmente requieran una mayor atención de parte del personal técnico que labora en esa dependencia.

El incumplimiento de las metas planificadas implicaría dificultad para establecer si los recursos asignados al CGI están siendo distribuidos y utilizados de forma eficiente y generando un impacto adecuado en los servicios de tecnologías de información y comunicaciones que se prestan a los usuarios internos del CAIS.

6. Sobre el inventario de componentes en stock para mantenimiento correctivo.

Mediante verificación física de los componentes almacenados en la bodega del CGI del CAIS de Siquirres, se detectaron el 9 de febrero de 2018, diferencias en relación con lo reportado en la base de datos del Sistemas SOS, mediante el cual se registran y atienden las solicitudes de soporte técnico de los usuarios de tecnologías de información, según se detalla a continuación:

[12] Entrevista escrita del 5 de marzo 2018

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

Cuadro 1
Diferencias inventario repuestos
CGI-CAIS Siquirres
2018

Componente	*Existencia reportada en SOS*	*Existencia Contabilizada*	*Diferencia*	*Costo Unitario*	*Costo Diferencia*
Adaptador de red inalámbrico USB	10	9	-1	10.000	10.000
CD-R	496	479	-20	NR	NR
Disco Duro-SATA	9	6	-3	67.020	201.060
Estabilizador y regulador de voltaje	25	17	-8	5.381	43.050
Fuente de poder	18	16	-2	8.000	16.000
Hub 24 puertos	5	4	-1	52.500	52.500
Memorias RAM	26	19	-7	14.060	98.423
Mouse óptico USB	14	13	-1	NR	NR
Tarjeta de video	2	1	-1	25.101	25.101

Fuente: Elaboración propia.

En oficio CAIS-2631-CGI-015-2018, el Msc. Deiler Calvo Matamoros, encargado del CGI del CAIS de Siquirres, indicó lo siguiente:

"*Conforme a resultados de las diferencias de saldos de existencia de dispositivos/componentes en bodega del Centro de Gestión Informática (CGI) del CAIS Siquirres y lo confirmado de estos resultados con su persona se detalla lo siguiente:*

1. *CD-R TDK: Grabados y utilizados por el CGI para contar con recursos para instalación aplicativos y soporte técnico. Asimismo, se han grabado archivos relacionados con la Oficina Financiero Contable del CAIS para gestión de modificaciones presupuestarias.*

2. *Disco duro-SATA Seagate: Utilizados en mejora tecnológica aplicada a equipos placa institucional 794445, 794440 y 794442.*

3. *Estabilizador y regulador de voltaje: Utilizados por el CGI para soporte técnico (4), además, dispositivos utilizados en puesto de trabajo de Encargada de Adquisiciones, Secretaria Adquisiciones, Coordinación de Enfermería I Nivel y Telemedicina.*

4. *Fuente de poder Full Power: Utilizada en equipo placa institucional 1004161.*

5. *Hub D-Link: Facilitado a CGI Regional en calidad de préstamo, actualmente en proceso de devolución.*

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

6. *Memoria RAM Kingston: Utilizadas en mejora tecnológica aplicada a equipos placa institucional 794445, 794440, 794442 y 800435.*

7. *Mouse óptico USB Microsoft: Utilizado con equipo placa institucional 1081450.*

8. *Tarjeta de video: Utilizada en equipo placa institucional 917596."*

El Modelo de Funcionamiento y Organización del Área de Gestión de Bienes y Servicios, en el apartado 9.4, de las funciones sustantivas para el desarrollo del Subproceso de Almacenamiento y Distribución, establece en los puntos 8 y 9 lo siguiente:

"*Controlar, registrar y documentar los movimientos y afectaciones que se realicen al inventario: entradas, salidas, altas, bajas, y otras, con base en los contratos, las órdenes de compra, las facturas, las actas, los pedidos, las devoluciones, los ajustes y las disposiciones administrativas, con el propósito de contar con información oportuna y veraz sobre las condiciones de los productos en custodia"*.

El Instructivo que regula los faltantes y sobrantes de activos y suministros de la Gerencia Financiera indica en su artículo 37:

"Prácticas y medidas para minimizar los faltantes y sobrantes de activos y suministros.

La administración de la Unidad Ejecutora debe diseñar medidas y prácticas de control interno las cuales deben adoptar sus funcionarios, para el enfrentamiento de los riesgos relevantes que pueden sufrir los activos y suministros de la Institución."

Ciertamente las diferencias evidenciadas en el inventario de componentes utilizados para el mantenimiento correctivo de los equipos de cómputo y comunicaciones en el CGI del CAIS de Siquirres fueron adecuadamente justificadas por el encargado Msc. Calvo Matamoros, no obstante, la situación descrita pone en evidencia debilidades en el registro de lo utilizado en la atención de las necesidades de los usuarios.

Esta circunstancia eleva el riesgo de extravío, pérdida o sustracción de suministros que han sido adquiridos con fondos institucionales y cuya función es la de contar con lo requerido para enfrentar la reparación de un equipo y no afectar la continuidad de los servicios.

7. Sobre la capacitación de los funcionarios del CGI

No se evidenció la participación de los funcionarios del CGI del CAIS de Siquirres en capacitaciones relacionadas con sus funciones sustantivas. Al respecto, y con la finalidad de ampliar los conocimientos en aspectos relacionados con la atención de la infraestructura de tecnologías del área, se ha incluido dentro de las especificaciones técnicas de las compras de servicios de mantenimiento del sistema de videovigilancia y del sistema de voz y datos, un apartado de capacitación por parte de los proveedores adjudicados; sin embargo, dichas actividades responden a un conocimiento específico de los objetos de la compra y atienden las necesidades identificadas con antelación en esta materia.

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 Centro de Gestión Informática del CAIS de Siquirres estableció en el documento denominado "Estudio de necesidades de bienes y servicios TIC 2016-2017", requerimientos relacionados con la capacitación de los funcionarios de esa unidad, en lo que interesa se indicó:

"*Considerados algunos procesos de mejora continua en los procesos TIC conlleva a que el personal se mantenga en constante actualización y previéndose de conocimiento de las últimas tecnologías y los entornos que lo rodea, es por ello que se requiere de capacitación en algunas áreas afines.*

Se requiere de administración en motores de bases de datos SQL Server dada la administración de sistemas como el SIFA, SIIP y SIIS. Por el otro lado se pretende fortalecer el conocimiento en el levantado de requerimientos para la adecuada gestión de proyectos y aseguramiento de la calidad, así como sensibilización e importancia del uso de las TIC a través de las computadoras. La seguridad informática es necesario ya que como personal encargado de las TIC es necesario afrontar las amenazas y vulnerabilidades que pueden afectar la red y poner en riesgos los recursos e información institucional, el tema de red es importante ya que permite administrar de manera idónea la plataforma de red instalada en el CAIS y ampliar el conocimiento en el tema, se solicita la capacitación en otros temas importantes en tema de administración de proyectos y virtualización ya que el incremento en recursos TIC, incremento en el personal a asistir, y la complejidad del área de salud como Centro de Atención Integral en Salud y sus diferentes EBAIS."

Los temas de capacitación que se determinaron como necesarios son: Introducción a las bases de datos con SQL Server, Administración en SQL Server 2012, Taller práctico de requerimientos interacción humano-computador, Ethical Hacking, Continuidad del negocio y recuperación de desastres, Configuración de redes CISCO CCNA 1 (fundamentos de redes), Cableado estructurado, Administración de proyectos con MS-Proyect, Virtualización–Vmware vSaphere: install-configure-

manage V. 6.0, Fundamento de gestión de proyectos de TI, Introducción a la virtualización, MS Project bajo estándar del PMI.

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.

Los funcionarios del CGI del CAIS de Siquirres enfrentan la administración de servidores de nivel de complejidad medio, así como de motores de bases de datos como SQL, procesos de continuidad del negocio y recuperación de servicios, configuración de redes CISCO, infraestructuras de voz y datos, por lo requieren de elementos que les permitan mantener actualizados sus conocimientos en todos estos temas, sin embargo, las gestiones que se han realizado por parte de las autoridades del CGI y del centro de salud, no han sido efectivas.

En contrario, la ausencia de programas de refrescamiento de los conocimientos eleva el riesgo de no poder hacer frente a situaciones que afecten la prestación de servicios de tecnologías y de información y ente el avance de herramientas como EDUS, impactando en el proceso de atención a los usuarios de servicios.

CONCLUSIÓN

El Centro de Gestión Informática del CAIS de Siquirres presenta oportunidades de mejora en los procesos relacionados con su gestión administrativa, tales como análisis determinación y valoración de riesgos, documentación y actualización de resultados de ensayos del plan de continuidad, capacitación de funcionarios, establecimiento y evaluación de indicadores de gestión, entre otros.

Las actividades operativas del CGI, ciertamente consumen un alto volumen de los recursos asignados, no obstante, no deberían ocasionar la no ejecución o postergación de los procesos administrativos, como la actualización de documentos que respaldan las acciones a ejecutar ante la materialización de alguno de los riesgos identificados previamente.

En lo referente a las diferencias evidenciadas en el inventario de dispositivos y componentes utilizados para efectuar mantenimiento correctivo de los equipos que no cuentan con garantía, es necesario indicar que responden en principio a debilidades de control en el registro de lo utilizado en cada caso, lo que evita que se conozca con exactitud las cantidades de cada uno de los insumos disponibles.

La planificación anual del CGI deben constituirse en la herramienta que permita verificar el avance y cumplimiento de metas que permitan potenciar la prestación de los servicios tecnológicos en beneficio de los usuarios internos y los asegurados, de forma tal se hace necesaria la revisión de las actividades incluidas, así como de los indicadores de gestión utilizados.

Finalmente, la capacitación del personal en temas de complejidad media facilita el crecimiento de las capacidades técnicas, redundando en mejor atención y una mejora en las propuestas de crecimiento de la plataforma técnica del área.

RECOMENDACIONES

AL LIC. ZIMRI CAMPOS QUESADA, ADMINISTRADOR DEL CENTRO DE ATENCIÓN INTEGRAL EN SALUD DE SIQUIRRES, O QUIEN EN SU LUGAR OCUPE EL CARGO.

1. De acuerdo con lo expuesto en el hallazgo 7, analizar las necesidades de capacitación del personal del CGI, incluidas en el "Estudio de Necesidades 2016-2017" a efectos de elaborar un plan que permita fortalecer los conocimientos y capacidades de los funcionarios de esa dependencia, el cual deberá ser incorporado en el Plan de Capacitación y Formación de esa unidad, de conformidad con el Reglamento de Capacitación y Formación de la Caja Costarricense de Seguro Social.

Plazo: 6 meses a partir del recibo del presente informe.

2. Según lo descrito en el hallazgo 1, en coordinación con el Centro de Gestión Informática, garantizar la definición formal de los procesos relevantes que ejecuta el Centro de Gestión Informática del CAIS de Siquirres, para efectos de acreditar el cumplimiento de esta recomendación, deberá remitirse a esta Auditoría, la documentación que respalde la identificación de los procesos relevantes, así como la aprobación correspondiente por parte de esa Administración.

Plazo: 8 meses a partir del recibo del presente informe.

3. A partir de lo indicado en el hallazgo 2, en coordinación con Centro de Gestión Informática, proceder con la actualización de los riesgos para la totalidad de la infraestructura y los servicios de tecnologías de información, así como con la identificación de aquellos que corresponden específicamente al Centro de Gestión Informática.

Plazo: 6 meses a partir del recibo del presente informe

4. De conformidad con la situación descrita en el hallazgo 3, garantizar en coordinación con el Centro de Gestión Informática, el establecimiento de los protocolos para la implementación de controles de seguridad de los recursos informáticos disponibles en el área de salud.

Plazo de cumplimiento 6 meses a partir del recibo del presente informe.

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

5. Establecer, en coordinación con el Centro de Gestión Informática, un cronograma de atención de las observaciones emitidas por la Sub Área de Continuidad de la Gestión de la Dirección de Tecnologías de información y Comunicaciones, mediante Documento SCGTIC-039-2016 "Informe sobre la evaluación del Plan de Continuidad de la Gestión TIC Área de Salud de Siquirres, E.U 2631"; debe contemplarse en ese cronograma el plazo de atención y responsable de ejecutar las acciones correspondientes para atender cada una de las observaciones del citado documento

Plazo: 6 meses a partir del recibo del presente informe.

6. En relación con la Planificación Anual, en coordinación con el Centro de Gestión Informática, efectuar un análisis que permita definir la pertinencia de los objetivos y actividades incluidos en la planificación del anual del CGI, así como la inclusión de indicadores de avance y cumplimiento de las metas establecidas. Para acreditar el cumplimiento de esta recomendación, deberá remitirse a esta Auditoría en un plazo de 6 meses el respaldo documental del análisis realizado.

7. Considerando los resultados del hallazgo 6, instruir al Centro de Gestión Informática lo siguiente:

a. Garantizar el registro oportuno en el sistema SOS de los insumos utilizados en labores de mantenimiento correctivo de los equipos.
b. Efectuar controles de inventario de manera periódica, con la finalidad de asegurar la utilización adecuada de los insumos.

Plazo: 1 mes a partir del recibo del 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 la Dra. Tania Ching Chang, Directora Médica, Lic. Zimri Campos Quesada, Administrador y Lic. Deiler Calvo Matamoros, Coordinador del Centro de Gestión Informática, todos del Área de Salud de Siquirres.

Respecto a la recomendación 2 el Lic. Campos Quesada solicitó ampliar el plazo a 8 meses, lo cual fue discutido y aceptado, el cambio se incorpora en el presente informe.

ÁREA GESTIÓN OPERATIVA

ALEXANDER ARAYA MORA (FIRMA)
Firmado digitalmente por ALEXANDER ARAYA MORA (FIRMA)
Fecha: 2018.05.09 14:26:15 -06'00'

MIGUEL ANGEL SALVATIERRA ROJAS (FIRMA)
Firmado digitalmente por MIGUEL ANGEL SALVATIERRA ROJAS (FIRMA)
Fecha: 2018.05.09 14:25:49 -06'00'

Br. Alexander Araya Mora
ASISTENTE DE AUDITORÍA

Ing. Miguel Ángel Salvatierra Rojas
JEFE DE SUBÁREA

MASR/AAM/wnq