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

ATIC-098-2022
22 de noviembre de 2022

RESUMEN EJECUTIVO

El estudio se realizó de conformidad con el Plan Anual de Trabajo 2022 de la Auditoría Interna, apartado actividades programadas, con el propósito de evaluar funcionalidad, implementación y operación del Sistema de Gestión de Archivo y Correspondencia (SAYC) a nivel institucional

Los resultados del presente informe evidencian oportunidades de mejora relacionadas con la documentación del proceso de desarrollo e implementación del SAYC ejecutado por el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías.

Aunado a lo anterior, se evidenció un retraso en el cumplimiento de las fases “Piloto Regional y Local” e “Implementación Regional y Local”, de uno y dos años respectivamente, lo que se refleja en un avance total del 85% en la implementación del proyecto y en aproximadamente 121 unidades pendientes de incluir que responden mayoritariamente a hospitales y áreas de salud.

Además, de un nivel de insatisfacción de los usuarios con la funcionalidad del sistema, en aspectos tales como: capacitación recibida, resolución de dudas, uso de herramientas paralelas al sistema, entre otros. Adicionalmente, se comprobó la carencia de mecanismos de contingencia formalmente establecidos que permitan la continuidad en caso de materialización de riesgos relacionados con la suspensión o afectación de servicios apoyados mediante la aplicación.

Finalmente, el SAYC dispone como medida de seguridad en el acceso únicamente con validación de usuario y contraseña, sin estar integrado al Módulo Integrado de Seguridad (MISE) ni otros mecanismos como factor doble de autenticación, tal como lo establece la normativa y mejores prácticas aplicables.

En virtud de los resultados se emiten 7 recomendaciones dirigidas a las autoridades de las Gerencias de Infraestructura y Tecnologías, y Administrativa con la finalidad de fortalecer los procesos relacionados con la implementación y desarrollo del Sistema de Archivo y Correspondencia.

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

ATIC-098-2022
22 de noviembre de 2022

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA FUNCIONALIDAD, IMPLEMENTACIÓN Y OPERACIÓN DEL SISTEMA DE GESTIÓN DE ARCHIVO Y CORRESPONDENCIA (SAYC) A NIVEL INSTITUCIONAL

ORIGEN DEL ESTUDIO

El presente estudio se realizó en atención al Plan Anual Operativo de la Auditoría Interna para el 2022, apartado de actividades programadas.

OBJETIVO GENERAL

Evaluar la funcionalidad, implementación y operación del Sistema de Gestión de Archivo y Correspondencia (SAYC) a nivel institucional.

OBJETIVOS ESPECÍFICOS

- Verificar el cumplimiento de la normativa institucional para el desarrollo e implementación del SAYC, de conformidad con lo establecido en la Metodología de Desarrollo de Sistemas.
- Comprobar el grado de implementación del SAYC a nivel institucional.
- Constatar los mecanismos de seguridad lógica desarrollados en el SAYC.
- Verificar que la funcionalidad del SAYC se ajuste a la atención de requerimientos de los usuarios.
- Analizar la frecuencia de incidencias y problemas de la aplicación.
- Identificar el diseño e implementación de mecanismos de contingencia en la gestión de correspondencia, ante la imposibilidad de utilización del SAYC.

ALCANCE

El estudio comprende el análisis de las acciones efectuadas por la Administración Activa en torno al desarrollo, implementación y operación del Sistema de Gestión de Archivo y Correspondencia (SAYC), en el periodo comprendido entre el 2021 y 2022, ampliándose en aquellos casos que se consideró necesario.

La evaluación se efectuó de acuerdo con lo dispuesto en las Normas Generales de Auditoría para el Sector Público y Normas para el Ejercicio de la Auditoría Sector Público, divulgadas a través de la Resolución R-DC-064-2014 de la Contraloría General de la República, publicadas en La Gaceta 184 del 25 de setiembre 2014, vigentes a partir del 1º de enero 2015 y demás normativa aplicable.

LIMITACIONES

Durante el desarrollo del estudio se presentaron limitaciones asociadas con la disponibilidad del personal encargado del desarrollo e implementación del SAYC destacado en el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías, lo cual llevó a interrumpir de manera temporal el análisis e incluso reducir el alcance de la evaluación.

Entre las situaciones más influyentes, se encuentra el ataque cibernético del 31 de mayo del 2022 perpetrado en la CCSS y sus efectos a partir de la desconexión de sistemas de información. En ese sentido, la Institución avocó sus esfuerzos al restablecimiento de los servicios tecnológicos, así como al fortalecimiento de los procesos críticos. Aunado a lo anterior, el acceso a la información de respaldo de las acciones ejecutadas por la administración fue limitado dado las afectaciones sufridas en los servidores de archivos, así como en las unidades de almacenamiento conectadas a la red (NAS).

METODOLOGÍA

Con el propósito de alcanzar los objetivos del presente estudio se aplicaron los siguientes procedimientos metodológicos:

- Revisión y análisis de documentación relacionada con el desarrollo, evolución funcional, implementación, estudios de factibilidad del SAYC.

- Revisión y análisis del Proyecto de Estandarización y Automatización de la Gestión de Correspondencia elaborado por la Gerencia Administrativa.

- Aplicación de encuesta de satisfacción de usuarios del SAYC.

- Sesiones de trabajo por medio de la herramienta institucional TEAMS con los funcionarios:

    - Ingeniero Giovanni Campos Alfaro, jefe del Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnología.
    - Ingeniero Gerardo Salazar González, jefe a.i del Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales

MARCO NORMATIVO

- Ley General de Control Interno, N° 8292, julio 2002.
- Normas de Control Interno para el Sector Público, R-CO-9-2009 Contraloría General de la República, febrero 2009.
- Normas Generales de Auditoría para el Sector Público, Resolución R-DC-064-2014, setiembre 2014.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021.
- Políticas Institucionales de Seguridad informática.
- Normas Institucionales de Seguridad Informática.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría informa y previene al Jerarca 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 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

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

ANTECEDENTES

1. **Informe de Auditoría ATIC-306-2014 "Estudio especial sobre la estandarización y automatización de la gestión y seguimiento de la correspondencia y asuntos institucionales".**

Esta Auditoría comunicó los resultados de evaluación sobre la gestión y seguimiento de la correspondencia y asuntos institucionales en el mencionado informe del 17 de diciembre de 2014. Como objetivos del estudio se definieron entre otros la verificación de las herramientas tecnológicas utilizadas por la Presidencia Ejecutiva y gerencias para el trámite, administración y seguimiento de la correspondencia institucional, además de verificar la existencia de una estrategia institucional para desarrollar la estandarización y automatización de este proceso, así como la indagación respecto a la definición de un sistema de correspondencia oficial a nivel institucional.

Los principales hallazgos del estudio se relacionaron con la ausencia de una estrategia institucional para la automatización y estandarización de la gestión de la correspondencia, dado que no se evidenciaron objetivos asociados a esta materia en el Plan Estratégico Institucional y el Plan Táctico de la Gerencia Administrativa.

Además, la institución en ese momento carecía de un proceso estandarizado que permitiera la administración del flujo de documentos (recepción, trámite, envío y seguimiento) de la correspondencia. Lo anterior basado en el análisis de los procedimientos ejecutados por Presidencia Ejecutiva, Gerencias de Pensiones, Infraestructura y Tecnologías, Administrativa, Financiera y Médica, así como la Sub Área de Archivo y Correspondencia unidad rectora en esa materia.

En línea con lo anterior, se determinó la ausencia de un sistema informático institucional oficial estandarizado que permita la gestión y seguimiento de la correspondencia para el soporte del proceso documental permitiendo obtener eficiencia y eficacia en los tiempos de entrega, trazabilidad control de documentos recibidos y emitidos. Al contrario, se evidenció la utilización de diversas herramientas para la ejecución de este proceso.

Finalmente, se verificaron aspectos relacionados con documentación, obsolescencia, involucramiento de la organización, usuarios que gestionen el desarrollo evolutivo y lideres funcionales del flujo de asuntos, de las herramientas tecnológicas desarrolladas por la Direccion de Tecnologías de Información y Comunicaciones para la gestión de la correspondencia que en ese momento

correspondía al Sistema de Seguimiento de Asuntos (SEGASU) y Sistema Gestor de Seguimiento y Control (GESC).

Al respecto se emitieron 4 recomendaciones dirigidas a la Presidencia Ejecutiva con la finalidad de conformar un equipo interdisciplinario, con la finalidad de estandarizar la gestión de la correspondencia así como su seguimiento; analizar los sistemas informáticos mencionados en el estudio y las otras herramientas disponibles en la institución para determinar la viabilidad de seleccionar alguna de ellas que reúna las condiciones adecuadas para la automatización, definir un plan de implementación de la solución tecnológica seleccionada y un proceso de transición que permitiera a los usuarios finales y las unidades institucionales realizar el cambio al sistema propuesto. Además, se solicitó a la Gerencia de Infraestructura y Tecnologías recordar a nivel institucional, la carecía de soporte técnico por parte de los analistas del Área de Ingeniería de Sistemas del SEGASU, provocando en ese momento un aumento de riesgos de seguridad de la información registrada en esa plataforma.

Como resultado de las acciones ejecutadas por la administración para la atención de las recomendaciones se elaboró el Plan de Estandarización y Automatización de la Gestión de la Correspondencia que se detalla seguidamente.

2. Plan de Estandarización y automatización de la Gestión de la Correspondencia.

En atención al informe de Auditoría mencionado se conformó un Comité Intergerencial que se abocó al desarrollo de las acciones para estandarizar el procedimiento de la Gestión de Correspondencia Institucional, entre las cuales se definieron los requerimientos del sistema de información en tres procesos a saber: Gestión de Correspondencia, Gestión de Archivo y Gestión de Asuntos.

Adicionalmente, se procedió al análisis de los sistemas de información utilizados en la institución en esos procesos, cuyo resultado permitió establecer que el utilizado en el despacho de la Gerencia de Infraestructura y Tecnologías (GIT) cumplía con los requerimientos evaluados.

En virtud de lo anterior, el Consejo de Presidencia y Gerentes en sesión del 4 de abril de 2016 aprobó la estrategia para estandarización y automatización de la Gestión de la Correspondencia Institucional, cuya implementación sería coordinada por la Gerencia Administrativa, así mismo el soporte y mantenimiento evolutivo del Sistema de Archivo y Correspondencia (SAYC) estaría a cargo del Centro de Gestión informática de la GIT, además se establecen dos etapas de implementación donde la primera corresponde a oficinas centrales y la segunda a la integración del nivel local y regional.

El plan detallaba 4 fases para su desarrollo que se detallan seguidamente.

- Fase I: Diagnóstico

  Tenía como objetivo disponer de un informe de diagnóstico de la situación actual de la organización, conclusiones y recomendaciones para realizar el plan de acción. Este proyecto constaba de dos líneas de acción, una para nivel central y otra para el nivel regional y local.

  Las actividades ejecutadas fueron:

  - Identificación de las unidades pendientes de implementar a nivel central, su flujo documental y cantidad de funcionarios a capacitar. En función de la información recopilada se procede al realizar el plan de trabajo a nivel central.

- Elaboración de diagnóstico de la situación actual en gestión de correspondencia en la unidad local y regional definida por el administrador del proyecto.

- Fase II: Planificación

  Buscaba establecer y acordar un plan de acción detallado de tareas y compromisos entre el personal asignado al proyecto y los patrocinadores de este. Además de las actividades, tiempos, productos y responsables del proyecto.

- Fase III: Ejecución

  Establecía como meta completar las actividades establecidas en el alcance del plan de acción y lograr los objetivos del proyecto para ello se apoya en las estrategias de estandarización y automatización:

  a. Gestión de correspondencia a nival central: con la identificación y posterior inclusión de las unidades ubicadas en oficinas centrales.

  b. Institucional: con la aplicación del plan piloto regional y local, se define la estrategia y de forma posterior la implementación.

- Fase IV: Implementación

  El objetivo era iniciar la puesta en marcha del proyecto, identificando los ajustes necesarios del sistema y procesos para ser incluidos como mejoras posteriores.

  a. Implantación en oficina centrales: incluir las unidades pendientes adscritas en oficinas centrales.

  b. Implementación regional y local: una vez definida la estrategia se lleva a cabo la implementación a nivel institucional.

- Fase V: Gestión del Cambio

  El proyecto elaboraría un informe con el plan de gestión de cambio basado en la definición de los objetivos, alcance, grupos de interés, direccionadores del cambio, actividades y cronograma de actividades.

- Fase VI: Conclusión

  Suponía una implementación en un periodo corto, la finalización esperada del proyecto se espera al cabo de 9 meses.

3. Selección del Sistema de Archivo y Correspondencia (SAYC) como herramienta institucional para la estandarización y automatización de la gestión documental.

El Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales adscrita a la Gerencia Administrativa, procedió durante el 2016 a la verificación de los sistemas de gestión de archivo y correspondencia en uso institucionalmente, basados en parámetros como:

- Aspectos Generales: Valoraba entre otros elementos la de integración con el MISE, correo electrónico y directorio activo, uso de certificados y firma digital, bitácoras para el control del proceso, genera diferentes perfiles de usuarios, uso de documentos en formato PDF, interacción de diferentes unidades, cumplía con la arquitectura institucional, valida ingreso por medio de usuario y contraseña, posee capacidad para altos flujos de documentos, permite búsquedas OCR.

- Gestión de la Correspondencia: consideraba aspectos como generación de número consecutivo, visualización de estado, generación de reportes detallados, adjuntar archivos, asociarlos a un expediente, establecer búsquedas por diferentes criterios, compartir información digitada en los módulos “Gestión de Archivos y Gestión de Asuntos”.

- Gestión de Archivo: se valoraron condiciones como generación, administración y control (abierto, cerrado, pasivo, reabierto) de expedientes digitales que pueda contener uno o varios documentos, disponer de un modo de consulta y acceso para múltiples funcionarios, genera foliatura y orden cronológico, permite grabar diferentes formatos de (docx, xlsx, jpg, mpg, avi), el sistema no produce copias de los documentos (trabaja con ubicaciones bajo punteros), genera alertas para los que pierden vigencia, posee restricción ilimitada en el tamaño de los archivos.

- Gestión de Asuntos: se consideraron aspectos como visualización de leído una vez asignado el asunto, generación de consecutivos de números de oficio para la elaboración de las notas de respuesta con su respectivo formulario y crearla desde la herramienta, permitía firma digital en distintos formatos y extensiones, enviar por correo un documento que se encuentre en el sistema de información, imprimirlo y exportarlo, crear seguimiento, asignación de tareas a uno o varios usuarios, anotaciones de avances, acciones, generación de asuntos independientes, inclusión de archivos relacionados, relación con varios usuarios, múltiples firmantes, generación de reportes por estado y rango de fechas y notificaciones de vencimiento.

Al respecto, fueron evaluados los sistemas SAYC, SUPEN, GEST, GD-VISION y SCC-GL, obteniéndose los siguientes resultados:

Tabla 1
Valoración de sistemas para la gestión de correspondencia
2016

Sistema	Aspectos Generales	Gestión de Correspondencia	Gestión de Archivo	Gestión de Asuntos	Nota Final
SAYC	24	15	25	35	99
SUPEN	27	15	6	45	93
GEST	19	2	14	26	61
GD-VISION	25	9	18	14	66
SCC-GL	12	6	0	22	40

Fuente: Archivo de valoración de sistemas para gestión de correspondencia Gerencia Administrativa.

Aunado a lo anterior, en sesión del Consejo de Presidencia y Gerentes del 4 de abril del 2016, en el artículo 3° se acordó:

> "*Se define el SAYC 3.0 como el sistema institucional para la gestión de la correspondencia, y se asigna a:*
>
> *a. La Gerencia de Infraestructura y Tecnologías como responsable de su mantenimiento evolutivo, correctivo y preventivo.*
> *b. La Gerencia Médica y la Gerencia Financiera, que acompañen a la Gerencia Administrativa, en la comunicación oportuna a las Direcciones Regionales y Directores Médicos para la buena coordinación de los trámites de sus unidades con el nivel central."*

Así mismo, en el artículo 4° se indicó:

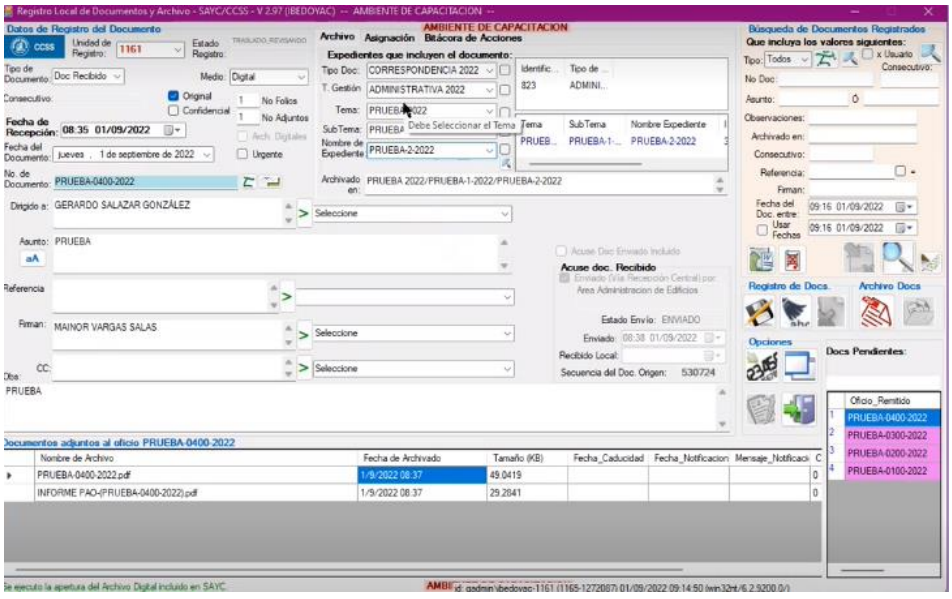
> *"Aprobar la estrategia y plan de acción presentados por el Comité Intergerencial para la implementación del SAYC 3.0 y estandarización de la correspondencia en su etapa I, la cual deberá ser coordinada por la Gerencia Administrativa, para lo cual:*
>
> *a. Los funcionarios del actual Comité Intergerencial pasarán de inmediato a conformar el Comité de Usuarios del SAYC 3.0.*
>
> *b. Cada Gerencia deberá asignar, en un plazo de 5 días hábiles, al menos un analista en sistemas TIC para bridar apoyo al proceso de implementación del SAYC.*
> *c. Las Gerencias Institucionales podrán apoyar el reforzamiento de la COIN según avances del plan de implementación, para lo cual deberá mediar solicitud y coordinación previa con la Gerencia Administrativa."*

4. Sistema de archivo y correspondencia (SYAC)

El Sistema de Archivo y Correspondencia fue desarrollado por el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías, inicialmente para la gestión de documentación interna, actualmente se compone de una aplicación en ambiente Windows, el cual se compone de los menús de Administración que permite la generación de usuarios, creación de catálogos, seguridad, entre otros, además de las opciones de gestión para correspondencia, asuntos, archivos y correo, entre otros.

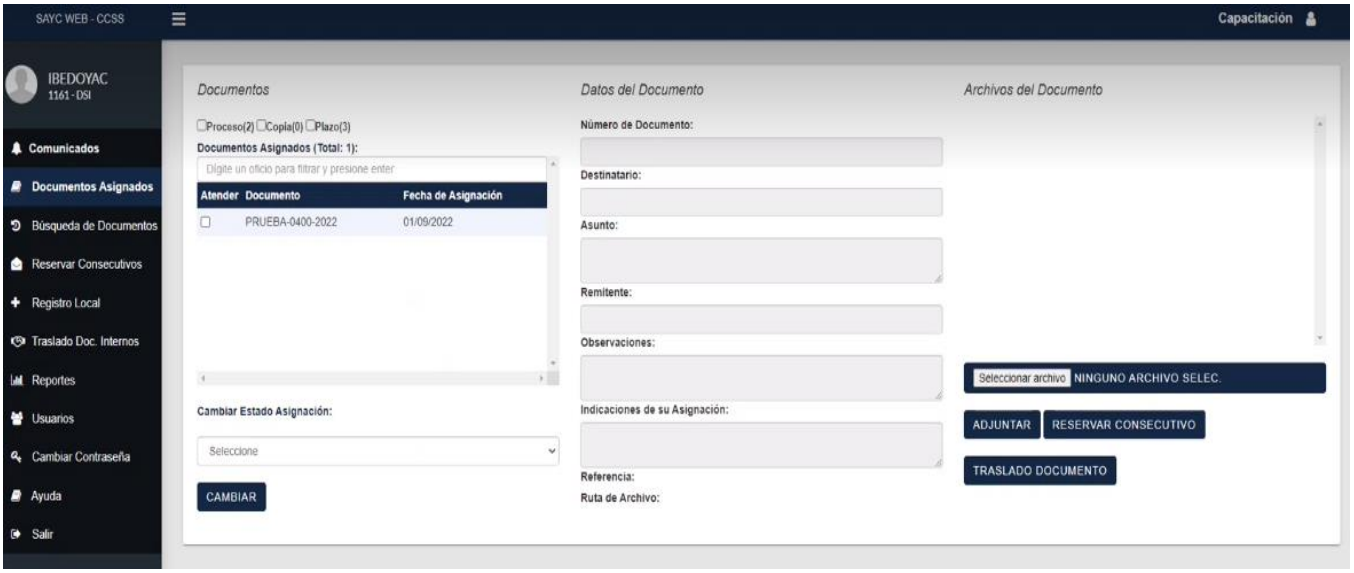
Imagen 1
Ventana de inicio SAYC

Imagen 2
Ventana Gestión de documentos SAYC



Adicionalmente, se desarrolló un módulo web para el uso de los usuarios finales permitiendo la consulta de los documentos asignados, búsquedas, traslados internos, entre otros. Dicho aplicativo complementa la funcionalidad de la aplicación Windows.

Imagen 3
Ventana Gestión documentos SAYC-WEB



HALLAZGOS

1. SOBRE LA DOCUMENTACIÓN QUE RESPALDA EL DESARROLLO E IMPLEMENTACION DEL SISTEMA DE ARCHIVO Y CORRESPONDENCIA.

Se evidenció que el Sistema de Archivo y Correspondencia (SAYC) cuenta con documentación parcial para su desarrollo y evolución según lo establecido en la Metodología de Desarrollo de Software de la Dirección de Tecnologías de Información y Comunicaciones. Lo anterior en virtud que únicamente se obtuvo evidencia de los siguientes productos:

- Aval para el desarrollo del sistema emitido por la Dirección de Tecnologías de Información y Comunicaciones.
- Aprobación por Consejo de Presidencia y Gerentes.
- Aprobación requerimientos de usuarios para versión web.
- Circular gerencia uso SAYC.
- Comunicados de funcionalidades nuevas.
- Cronograma del proyecto.
- Minuta de estandarización de la metodología de desarrollo.
- Gestión de pruebas funcionales e informe a gerencias versión web.
- Informe estado general del proyecto.
- Minutas de sesiones de trabajo para atención de requerimientos con usuarios.
- Modelo de base de datos.
- Roles y procesos de desarrollo y evolución.
- Estudio de factibilidad.

En virtud de lo anterior, no se obtuvo evidencia sobre la elaboración de los productos esperados para cada una de las fases establecidas en la Metodología de Desarrollo de Software de la Dirección de

Tecnologías de Información y Comunicaciones, la cual define al menos la generación de los siguientes documentos:

Tabla 2
Documentos incluidos en Metodología de Desarrollo de Software
Dirección de Tecnologías de Información y Comunicaciones

Fase	Documento
Conceptualización	Formulario de Inventario para Aplicaciones
	Glosario del Negocio
	Documento de Visión
	Diagrama de Casos de uso
	Lista de Casos de Uso para gestión de complejidad, riesgo y prioridad desde el punto de vista del usuario.
	Matices de funcionalidad: Necesidades vrs funcionalidades; funcionalidades vrs casos de uso
	Especificaciones Suplementarias
Elaboración	Especificación de casos de uso
	Plan de Pruebas
	Prototipo de Plan de Usuarios
	Modelo de solución UML
	Documento de Arquitectura de Software
	Modelo de bases de datos certificado
Construcción	Código Fuente
	Manual de Usuario
	Ayudas en Línea
	Documento de Transferencia Tecnológica
	Documento de resultado de pruebas de iteración
Transición	Manual de instalación y configuración
	Solicitud de bases de datos
	Gestión de tables e índices
	Documento de Puesta en Marcha de la aplicación
	Solicitud de paso a producción
	Plan de capacitación
	Plan piloto
	Resultados de capacitación
	Resultado de ejecución de plan piloto

Fuente: Metodología de Desarrollo de Software 2011, Dirección de Tecnologías de Información y Comunicaciones.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en su apartado X “Desarrollo, Implementación y Mantenimiento de Sistemas de Información” establece:

> *“La Unidad de TI debe aplicar practicas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo,*

realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida. La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones.

La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales. La Unidad de TI debe aplicar las prácticas de aseguramiento del cumplimiento contractual y las prácticas de calidad asociadas para los casos en utilice soluciones desarrolladas y/o implementadas por proveedores externos."

Las Normas Institucionales en Tecnologías de Información y Comunicaciones, en el apartado 3,2 Implementación de Software, establece en lo que interesa:

"Toda Área de trabajo debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe: (…)

- *Aplicar lo establecido en la Metodología de Desarrollo de Software, que considera la definición de requerimientos, los estudios de viabilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos.*
- *Aplicar lo establecido en la Metodología de Modelación de Datos Institucional.*
- *Contar con la debida Certificación de Cumplimiento con el Modelo de Datos Institucional que otorga la Dirección de Tecnologías de Información y Comunicaciones, con el propósito de integrar el modelo de datos la arquitectura de información de la Institución.*
- *Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software."*

El Ing. Giovanni Campos Alfaro, jefe del Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnología, indicó[1]:

"(…) debido a las afectaciones resultantes del ciberataque no estaban disponibles los archivos que respaldan el desarrollo del SAYC, dado que no se tenía acceso a los servidores de archivos ni a las unidades de almacenamiento en la red (NAS), de forma tal que forma era materialmente imposible atender los requerimientos hechos por la Auditoría".

Posteriormente el Ing. Campos Alfaro envío por correo electrónico los documentos mencionados anteriormente.

[1] En sesión de trabajo virtual mediante la plataforma institucional TEAMS del 26 de agosto del 2022.

El desarrollo de un sistema de información requiere de un proceso de construcción sistemática, organizada en diversas tareas y fases que aseguren la consecución de un producto final de calidad y de satisfacción a las necesidades de los usuarios, con ese fin se ha desarrollado institucionalmente la Metodología de Desarrollo de Software, que busca orientar a los responsables de esa tarea, mediante la aplicación de las mejores prácticas en esa materia.

En ese contexto, se debe indicar que la carencia de la documentación de respaldo del desarrollo del Sistema de Archivo y Correspondencia, así como de cualquier proyecto de desarrollo e implementación de soluciones de software de carácter institucional compromete la calidad del producto final, al adolecer de elementos que aseguren la atención adecuada de elementos tales como; requerimientos iniciales, diseño de base de datos, casos de uso, matrices de funcionalidad, entre otros, adicionalmente se desconoce la aplicación de las mejores prácticas en esta materia.

Ciertamente, la afectación sufrida por la institución en su infraestructura de almacenamiento de información por el ciberataque del 31 de mayo 2022, se constituye en un elemento limitante para el acceso a los datos que permitan evidenciar el cumplimiento total de la metodología de desarrollo, esta Auditoría considera necesario se proceda a su eventual recuperación o en dado caso a su reconstrucción.

2. SOBRE EL CUMPLIMIENTO DEL CRONOGRAMA DE IMPLEMENTACIÓN REGIONAL Y LOCAL.

Se evidenció que el proyecto de estandarización y automatización de la Gestión Documental incluyendo la implementación del Sistema de Archivo y Correspondencia tiene un avance total del 85%, no obstante, la última fase correspondiente a su implementación en el nivel regional y local tenía programada su finalización en noviembre del 2021, encontrándose actualmente 121 unidades pendientes en esa fase, mayoritariamente hospitales y área de salud.

Lo anterior de acuerdo con las actividades y plazos establecidos en el documento denominado: “Cronograma Proyecto estandarización y automatización Gestión Correspondencia Institucional”, el cual detalla las tareas a ejecutar para completar la implementación del SAYC en toda la institución.

De tal forma, el componente denominado: “Plan Piloto Regional y Local” muestra un avance parcial, estando pendiente la finalización del plan piloto y la elaboración, validación y aprobación del informe de implementación de esta etapa, según se muestra seguidamente:

Tabla 3
Avance del Plan Piloto Regional y Local
Sistema de Archivo y Correspondencia
Gerencia Administrativa
Agosto 2022

	Fecha Inicio Programada	Fecha Finalización Programada	Fecha Entrega Real
Fase: Plan Piloto Regional y Local			
Identificar la situación actual de las unidades	01-09-2019	31-12-2019	31-03-2020
Diseñar metodología y unidades de plan piloto	01-12-2019	31-12-2019	31-03-2020
Ejecutar Plan Piloto	01-01-2020	31-05-2020	No indicado
Elaborar informe Plan Piloto	01-06-2020	31-06-2020	No indicado
Revisar y validad informe de implementación	01-06-2020	31-06-2020	No indicado

Aprobar informe de Implementación	01-06-2020	31-06-2020	No indicado

Fuente: Cronograma Proyecto estandarización y automatización Gestión Correspondencia Institucional, Gerencia Administrativa.

Como consecuencia de lo anterior, la fase “Implementación Regional y Local” también muestra un retraso en la inclusión de las unidades que corresponden a ese nivel, así como en todas las actividades que la conforman; es necesario indicar que la implementación de este proyecto debía finalizar en diciembre del 2021, por lo que se evidencia un retraso de aproximadamente un año en su ejecución.

El detalle de la descrito se muestra seguidamente:

Tabla 4
Avance Implementación Regional y Local
Sistema de Archivo y Correspondencia
Gerencia Administrativa
Agosto 2022

Fase	Fecha Inicio Programada	Fecha Finalización Programada	Fecha Entrega Real
Implementación Regional y Local			
Definir estrategia de implementación institucional	01-07-2020	31-07-2020	No Indicado
Revisar y validar estrategia de Implementación	01-07-2020	31-07-2020	No Indicado
Aprobar estrategia de Implementación	01-07-2020	31-07-2020	No Indicado
Presentar estrategia a Consejo	01-07-2020	31-07-2020	No Indicado
Implementar la estrategia a nivel institucional (según plan de trabajo)	01-08-2020	31-11-2021	No Indicado
Informe de implementación	01-12-2021	31-12-2021	No Indicado

Fuente: Cronograma Proyecto estandarización y automatización Gestión Correspondencia Institucional, Gerencia Administrativa.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en su apartado X “Desarrollo, Implementación y Mantenimiento de Sistemas de Información” establece:

> *“La Unidad de TI debe aplicar practicas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida. La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones.”*

Sobre la situación descrita el Ing. Gerardo Salazar González, jefe a.i del Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales, en sesión de trabajo sostenida mediante videoconferencia por medio de la herramienta institucional TEAMS, indicó:

> *"Los retrasos en la implementación son resultado de diversos eventos que han afectado el ritmo de implementación en el nivel regional y local, entre ellos la cantidad de requerimientos necesarios para ajustar la aplicación a esos niveles, además, los esfuerzos institucionales fueron dedicados primeramente a la atención de la pandemia*

por COVID-19 y recientemente por la suspensión de los servicios de tecnologías de información y comunicaciones resultado de ataque cibernético de mayo de 2022."

Lo descrito ha ocasionado que el proyecto de estandarización y automatización de la gestión documental presente un retraso de aproximadamente dos años en la ejecución del componente "Plan Piloto Regional y Local" y un año en "Implementación Regional y Local", impidiendo la materialización del objetivo principal de este proyecto como lo es la integración institucional de gestión documental y asuntos en una sola herramienta, de tal manera a la fecha del presente informe aún está pendiente la inclusión de al menos 121 unidades entre las cuales se encuentran hospitales y área de salud, así como tres en el nivel central, entre ellas esta Auditoría, condicionando el traslado y atención de los requerimientos documentales entre las unidades usuarias del sistema y aquellas que aún no lo tienen.

Aunado a lo anterior, se debe señalar la persistencia de riesgos asociados con la estandarización e integración institucional del proceso, así como en la trazabilidad de los documentos originados en las unidades fuera del sistema, afectando la oportunidad en la atención y comprometiendo la responsabilidad de los funcionarios encargados de responder o atender los asuntos comunicados.

3. SOBRE LA SATISFACCIÓN DE LOS USUARIOS DEL SAYC.

De acuerdo con los resultados obtenidos en encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia, se identificaron oportunidades de mejora relacionadas con la satisfacción de los usuarios en aspectos tales como: capacitación de los usuarios, tipo de capacitación recibida, a quién recurre en caso de dudas, en qué plazo se resuelven las dudas o consultas, contingencia utilizada en caso de fallas del sistema, control y seguimiento de los documentos y asuntos, indicadores de gestión, entre otros los resultados se detallan seguidamente.

- Sobre la versión más utilizada, se tiene que la mayoría utiliza el sistema en su componente Web que tiene al momento 336 usuarios en tanto la versión escritorio cuenta con 194 y se registran 80 que usan ambas:

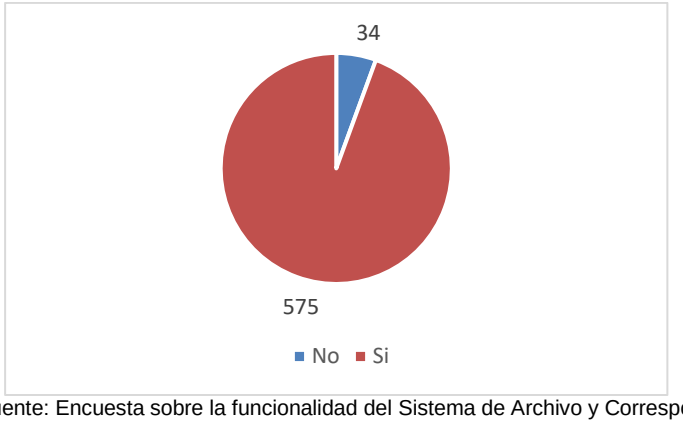
Tabla 5
Usuario por versión SAYC
Gerencia Administrativa
Octubre 2022

Tipo de sistema	Total de usuarios
Versión Web	336
Ambas	194
Versión de Escritorio	80

Fuente: Formulario sobre funcionalidad del SAYC, elaboración propia

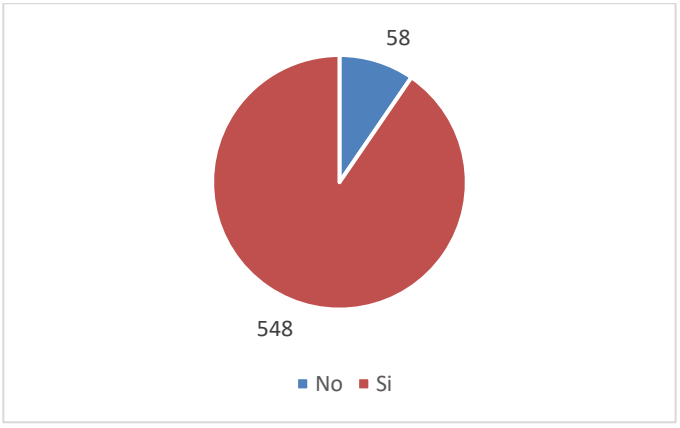
- Respecto a si el Sistema permite una gestión de archivos y correspondencia adecuada para la unidad, 575 usuarios se manifestaron positivamente, en tanto 34 indicaron que no, aunado a lo anterior 548 indicaron que el sistema facilita el seguimiento de los documentos y asuntos de la unidad, mientras 58 mencionaron que no, según se muestra seguidamente.

Gráfico 1
Gestión de Correspondencia
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

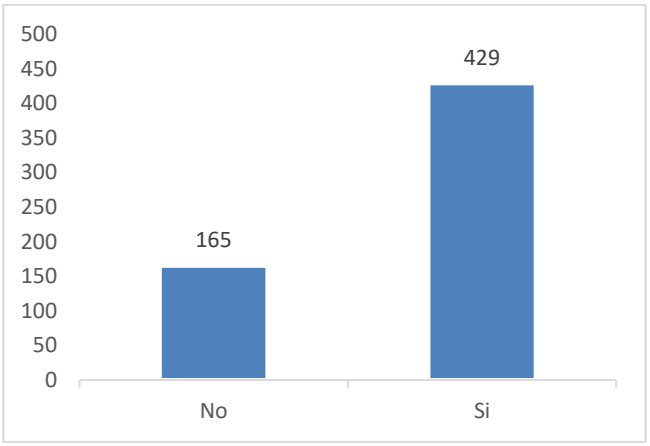
Gráfico 2
Seguimiento y control de documentos
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

- En relación con la posibilidad de generar indicadores de gestión relacionados con la correspondencia enviada y recibida, la percepción mayoritaria de los usuarios es que el sistema lo permite. No obstante 165 funcionarios indicaron una percepción negativa al respecto.

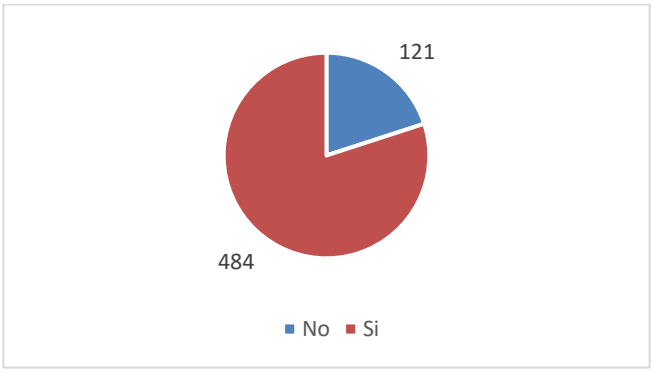
Gráfico 3
Generación de indicadores de gestión
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

- Respecto a la satisfacción de las necesidades en la gestión de correspondencia de la unidad, 121 usuarios indicaron percepción negativa, en tanto 484 mencionaron que si las satisface.

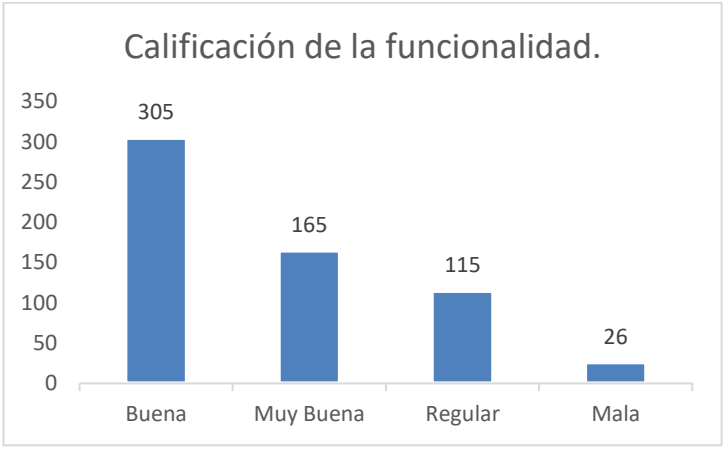
Gráfico 5
Satisfacción de las necesidades de la unidad
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

- Sobre la valoración que dan los usuarios a la funcionalidad del sistema, 141 la consideran entre regular y mala, como se muestra seguidamente:

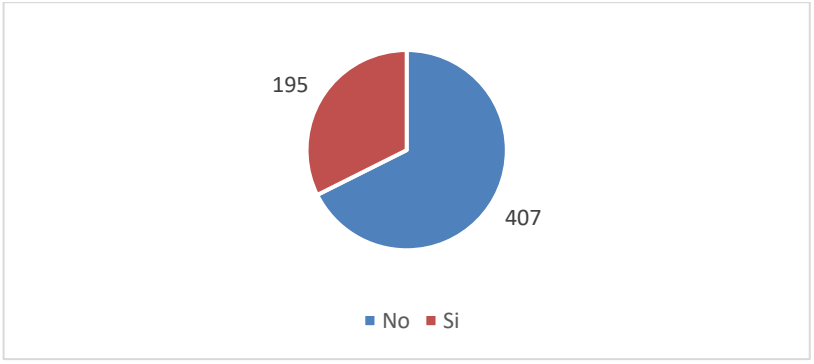
Gráfico 6
Valoración de funcionalidad del sistema
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

- Adicionalmente se consultó a los usuarios si la unidad utilizaba una herramienta adicional al SAYC para el control de la gestión documental, a lo que 195 respondieron positivamente, en tanto 407 de forma negativa. Las otras herramientas mencionadas fueron archivo de Excel con diversas modificaciones, archivo físico, almacenamiento en carpetas compartidas, consecutivo manual y carpeta compartida, CODI (sistema de archivo antiguo), correo electrónico, libros de actas y controles manuales, entre otros.

Gráfico 7
Uso de otras herramientas para gestión de correspondencia
Según usuarios SAYC



Fuente: Encuesta sobre la funcionalidad del Sistema de Archivo y Correspondencia

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en su apartado VI “Calidad de los Procesos Tecnológicos” establece:

> *“La institución debe implementar prácticas que permitan controlar los procesos organizacionales, posibilitando la mejora continua de productos y servicios, buscando asegurar la satisfacción de las necesidades institucionales, manteniendo estándares de documentación*

de los lineamientos requeridos, esquemas para la medición del desempeño y control sobre la vigencia de las practicas aplicables a los procesos.

Igualmente, debe generar servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo de los procesos que habilitan la gestión de las tecnologías de información."

La situación descrita, se origina en la percepción de atención sobre las necesidades de gestión documental en las unidades usuarias, que responde tanto a aspectos tales como; la implementación de un sistema nuevo, así como a los ajustes requeridos en el proceso, esta condición además se refuerza en la necesidad de comunicar las ventajas de la estandarización y automatización en la gestión y atención de los documentos y asuntos a nivel institucional.

Ciertamente la satisfacción de los usuarios de un sistema de información es alcanzada mediante la atención de los requerimientos de estos en relación con la funcionalidad de la aplicación, así como estableciendo mecanismos de coordinación y comunicación efectivos entre las partes involucradas. Respecto a los usuarios del SAYC, manifiestan inconformidades tanto en aspectos como funcionalidad, manejo de archivos, generación de indicadores de gestión e incluso se utilizan otras herramientas para la gestión documentos, duplicando los esfuerzos de registro y control de la información, ocasionando eventuales riesgos en la gestión documental al no contar con una valoración satisfactoria por parte de los usuarios, manifestándose en aspectos como uso inadecuado, limitada calidad de la información incluida, retrasos en la atención de asuntos, entre otros.

4. SOBRE LA CAPACITACIÓN DE LOS USUARIOS DEL SAYC.

Se evidenciaron oportunidades de mejora en la capacitación brindada para el uso del SAYC, lo anterior de acuerdo con lo expresado por 134 funcionarios en la encuesta mencionada anteriormente, que entre otros aspectos indican no haber recibido capacitación, haber aprendido consultado con otro personal de forma autodidacta. Adicionalmente, los usuarios indicaron desconocer los manuales de usuario del sistema.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en su apartado VII Recursos Humanos" indica:

"La institución debe disponer de un proceso formal que le permita gestionar los recursos humanos de acuerdo con las necesidades institucionales, en apego a directrices y regulaciones según aplique. Las practicas deben apoyar el reclutamiento, selección, contratación, inducción y capacitación continua según lo requerido. De igual forma, disponer de modelos que permitan la evaluación del desempeño de los funcionarios y la identificación de funcionarios con responsabilidades críticas y el desarrollo de habilidades en otros colegas que permitan sustituciones para asegurar la continuidad del servicio de las actividades principales."

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

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

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

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

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

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

Al respecto el Ing. Gerardo Salazar González, jefe a.i del Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales, en sesión de trabajo sostenida[2] mediante videoconferencia por medio de la herramienta institucional TEAMS, indicó:

> *"Como parte del proceso de implementación del sistema en las unidades se imparte una capacitación general sobre su uso, además de contar con la colaboración de funcionarios denominados enlaces, quienes tiene un nivel mayor de conocimiento de la herramienta y se encarga en primera instancia de atender las consultas y necesidades de información de los usuarios locales, adicionalmente, se cuenta con una serie de manuales de usuario y videos en la web de la institución para la satisfacción de las consultas."*

La capacitación en el uso de los sistemas institucionales busca que los usuarios comprendan su funcionamiento, así como su uso adecuado evitando la inclusión de datos erróneos y asegurando la calidad de la información almacenada y posteriormente utilizada para la toma de decisiones. Adicionalmente, al establecer herramientas y procesos permanentes en esta materia con la finalidad de recordar las funcionalidades e introducir las novedades en el sistema, permitirá una mejor adopción de la aplicación y disminución en la resistencia a su uso, así como el aseguramiento de la integridad de datos gestionados.

5. SOBRE LOS MECANISMOS DE CONTINGENCIA EN LA GESTIÓN DE LA CORRESPONDENCIA.

Se evidenció que el proceso de gestión de archivos y correspondencia carece de mecanismos de contingencia formalmente establecidos, que permita la continuidad de servicios ante la interrupción en la operación de la aplicación informática para el SAYC a nivel institucional.

[2] Sesión de trabajo virtual del 29 de agosto de 2022.

Además, en caso de presentarse esta circunstancia no se ha establecido un proceso estandarizado para la gestión documental en caso de no disponer del sistema, ya que existen unidades con diversos mecanismos adicionales al SAYC para controlar el flujo documental tales como; el uso de correo institucional, plantilla en Excel, uso de consecutivos internos, archivo de control de notificaciones, correo electrónico y en forma física.

De forma tal, los usuarios del sistema SAYC, mediante el formulario denominado: "Funcionalidad del sistema de Archivo y Correspondencia" aplicado por esta Auditoría, manifestaron lo siguiente con respecto al método de contingencia a utilizar eventualmente:

- "*Por medio de correo electrónico*".
- *"Utilizar números de consecutivos interno".*
- *"Se realizan hojas de Excel y se envían los oficios por correo electrónico."*
- *"Mediante correo electrónico, así como el archivo de control de las notificaciones realizadas"*
- *"Ninguna técnica debidamente establecida, se trabaja por asignación correo y de forma física"*
- *"Para enviar oficio se realiza listado consecutivo en papel y recibir desconozco".*
- *"Lo desconozco dado que se gestiona por el Despacho de la Gerencia, pero por ejemplo durante el ciberataque se no remitía por correo".*
- *"Para cualquier falla del SAYC desconozco el protocolo al respecto. En el evento reciente de la desconexión por hackeo, observé que se nombró a una secretaria ejecutiva, que coordinaba las acciones de envío y recepción de correspondencia. Supongo que con el apoyo del resto de secretarias de la Dirección."*

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en su apartado XIII "Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos" establecen:

> *"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
>
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."*

Sobre la situación descrita el Ing. Gerardo Salazar González, jefe a.i del Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales, en sesión de trabajo sostenida[3] mediante videoconferencia por medio de la herramienta institucional TEAMS, comentó:

> *"Ante la suspensión de los servicios prestados por el SAYC, se implementó un procedimiento de contingencia que requería la creación de carpetas digitales y asignación de permisos de acceso para la gestión de la documentación, no obstante, al tener una cantidad mayor de 400 unidades usuarios, su implementación no fue exitosa."*

La carencia de mecanismos de contingencia en la gestión documental institucional compromete la atención oportuna de los diversos asuntos que se tramitan por esa vía, así como la comunicación efectiva de múltiples asuntos a nivel interno, dada la suspensión en la continuidad de los servicios prestados por el sistema, en detrimento de aspectos de seguridad en la información y oportunidad en la atención de asuntos comunicados.

6. SOBRE LA SEGURIDAD EN EL ACCESO AL SAYC.

Se evidenció que el Sistema de Archivo y Correspondencia dispone como medida de seguridad únicamente del acceso con validación de usuario y contraseña propio de la aplicación, dado que no está integrado con el Módulo de Seguridad (MISE) institucional. Además, carece de otros mecanismos de tales como; doble factor de autenticación, accesos seguros, cambios periódicos y obligatorios de contraseña, políticas de inactividad de usuarios, entre otras prácticas de seguridad y validación.

El artículo 8 de la Ley General de Control Interno, respecto al sistema de control interno, establece:

> *"(…) 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, irregularidad o acto ilegal.*
> *b) Exigir confiabilidad y oportunidad de la información.*
> *c) Garantizar eficiencia y eficacia de las operaciones."*

Adicionalmente, las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente al apartado XI Seguridad y Ciberseguridad, indica:

> *"La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.*

[3] Sesión de trabajo virtual del 29 de agosto de 2022.

En ese contexto las Políticas Institucionales de Seguridad Informática, en su apartado 9.4 “PSI-CAR-004 Política utilización del Módulo Integrado de Seguridad (MISE) en los Sistemas de Información de la CCSS”, establece:

> *“El Módulo Integrado de Seguridad por sus siglas (MISE), es un sistema que brinda servicios de seguridad a las aplicaciones desarrolladas, el mismo administra lo relacionado con cuentas de usuarios, perfiles, permisos en los diferentes módulos y componentes de aplicaciones, de modo que los nuevos desarrollos realizados en la institución o contratados, no tendrán que desarrollar individualmente un módulo de seguridad, sino que podrán utilizar los servicios del MISE, lo que si deben considerar los nuevos desarrollos de aplicaciones es la conectividad con el Módulo Integrado de Seguridad.*
>
> *La utilización generalizada del Módulo Integrado de Seguridad “MISE”, en las aplicaciones desarrolladas en la CCSS, así como las contratadas externamente, es de suma importancia para salvaguardar la información, la continuidad del negocio y la no generación de problemas por pérdida de imagen. Por lo tanto, el Módulo Integrado de Seguridad, deberá ser utilizado de manera obligatoria en todos los desarrollos realizados en la institución así como los contratados, considerando que el mismo se instala y funciona en forma independiente de la aplicación de usuario, manteniendo una estrecha relación con la aplicación de usuario final, al compartir las bases de datos que administran la seguridad.”*

Así mismo, la Metodología para el Desarrollo de Software institucional, en su apartado de 3 “Fase de Construcción”, como parte de las tareas a desarrollar establece:

> *“4. Integración del sistema con el MISE: Según las políticas del Área Ingeniería de Sistemas, el Módulo Integrado de Seguridad (MISE) es el encargado de administrar la seguridad del sistema. Mediante este Módulo, se podrá definir la autenticación y autorización del Sistema. Para el proceso de integración con el MISE se debe seguir la Guía de integración del MISE con otros sistemas.”*

El Ing. Giovanni Campos Alfaro, jefe del Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnología, manifestó[4]:

> *“El desarrollo del sistema inicio aproximadamente en el año 2015 como una herramienta de uso interno de la Gerencia de Infraestructura y Tecnologías, de forma tal que no se consideró la necesidad de integrarlo al MISE”.*

Resulta pertinente indicar que la disminución de los riesgos asociados a la seguridad informática y ciberseguridad en distintos ámbitos institucionales debe considerar la posibilidad de dotar de diversos mecanismos de autenticación de los usuarios de los sistemas en uso, en este caso particular resulta necesario indicar que incluso carece de integración al MISE, debilitando la aplicación de políticas y modelos de seguridad implementados en esa herramienta. Esta condición adquiere mayor relevancia ante los eventos manifestados el 31 de mayo de 2022 a nivel institucional.

[4] En sesión de trabajo virtual mediante la plataforma institucional TEAMS del 26 de agosto del 2022.

7. SOBRE LA INFORMACIÓN NO INCLUIDA EN EL SISTEMA EN EL PERIODO DE INTERRUPCIÓN DE SERVICIO ANTE EL CIBERATAQUE.

Como resultado del ciberataque sufrido por la institución el 31 de mayo de 2022, fueron suspendidos los servicios informáticos institucionales, entre los que se encontraba la operación del Sistema de Archivo y Correspondencia, cuya operación fue retomada con normalidad en el mes de agosto de 2022.

Lo anterior representa un periodo de aproximadamente 3 meses de información gestionada por otros medios, lo cual provocó el eventual no registro en SAYC de aproximadamente 38.160[5] documentos mensuales. En ese sentido, no se obtuvo evidencia documental respecto a la formalización de una estrategia o metodología orientada a promover la inclusión de los datos mencionados con el fin de garantizar la integridad y completitud de la información en el sistema.

Al respecto, esta Auditoría señaló mediante el oficio AS-ATIC-133-2022, la necesidad de que los responsables de los sistemas de información establezcan acciones en torno a la incorporación de la información generada en ese periodo de contingencia en los sistemas de información correspondientes.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones, apartado “Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos”, cita:

> *“La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
>
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción.”*

Al respecto el Ing. Gerardo Salazar González, jefe a.i del Área de Publicaciones e Impresos de la Dirección de Servicios Institucionales, indicó[6]:

> *“Durante la atención de la emergencia provocada por el ciberataque se implementaron medidas de contingencia en los cuales se consideró la utilización de carpetas para el trámite de los documentos, adicionalmente se creó una herramienta para la inclusión de los oficios en las*

[5] Total de oficios tramitados durante al 30 de agosto de 2021: 387 556
[6] Mediante cédula narrativa del 7 de noviembre 2022.

unidades, no obstante, ambos resultaron poco funcionales, en caso de la herramienta automatizada requería el registro tanto de los documentos recibidos como enviados, asignación y atención, además se puso a disposición de las unidades aproximadamente 22 días antes de la puesta en marcha del SAYC. En ese contexto se preparó una guía para la inclusión de los documentos y se comunicó a las unidades usuarias, sin embargo, no se procedió al seguimiento de la situación dado que la información es propiedad de cada unidad.

No disponer de toda la información requerida en un sistema eleva la posibilidad de presencia de riesgos relacionados con el buen uso y funcionamiento del aplicativo y, por ende, del proceso que automatiza o digitaliza, en virtud de la afectación a la integridad de los datos, cuyo aspecto forma parte de los componentes fundamentales de la seguridad de la información. Asimismo, se disminuye la posibilidad de garantizar la trazabilidad de las transacciones, así como la confiabilidad de los datos para toma de decisiones.

CONCLUSIÓN

El desarrollo de sistemas a nivel institucional tiene como uno de sus objetivos lograr una mayor eficiencia en los procesos que se automatizan, desde esta perspectiva el establecimiento de una metodología de desarrollo está sustentada en la necesidad de definir un marco de referencia para la planeación y control de todo el proceso.

Ese marco tiene entre otras características el aseguramiento de la uniformidad y calidad de las actividades de desarrollo y del sistema, asegurar la satisfacción de las necesidades de los usuarios, lograr un mayor rendimiento y eficiencia de los funcionarios asignados al desarrollo de la aplicación, ajustarse a los plazos establecidos y a los costos previstos, generar de forma adecuada la documentación relacionada con el sistema y facilitar el mantenimiento posterior.

En ese contexto, el Sistema de Archivo y Correspondencia como componente de la estrategia para la estandarización y automatización de la Gestión de la Correspondencia fue aprobado como sistema institucional por el Consejo de Presidencia y Gerentes en sesión del 4 de abril de 2016, y a partir de ese momento se ha constituido en la herramienta institucional para el manejo de la documentación recibida y enviada a las diferentes unidades constituyendo un pilar fundamental en la atención oportuna de asuntos y casos por abordar, comunicación de disposiciones internas, entre otros aspectos de importancia institucional.

La documentación del desarrollo del sistema es relevante, considerando que respalda el cumplimiento de los requerimientos iniciales, asegura la calidad del producto entregado y permite establecer su ajuste a los modelos de bases de datos e información institucional y facilita el mantenimiento y evolución posterior.

Ciertamente, el desarrollo del SAYC inicio alrededor del año 2016 como una herramienta de uso local de la Gerencia de Infraestructura y Tecnologías, su adopción a nivel institucional obliga a considerar la documentación total del proyecto.

Adicionalmente, el proyecto de implementación muestra un retraso en sus fases de Plan Piloto e Implementación Regional y Local de dos y un año respectivamente, implicando que las unidades ubicadas en ese segmento de la institución aún no dispongan del sistema y recurran a otras herramientas para la gestión documental y atención de los asuntos asignados o comunicados.

Aunado a lo anterior, se ha manifestado insatisfacción con la funcionalidad y la atención de los requerimientos de gestión de las unidades, señalándose entre otros aspectos una valoración regular del sistema, carencia de indicadores de gestión, dificultad en el manejo de archivos, además de la persistencia de otras herramientas locales para la gestión documental, lo que implica un doble esfuerzo local de registro y control de la información y eleva el espacio lógico de almacenamiento.

Finalmente, es necesario señalar la importancia de disponer de mecanismos de contingencia estandarizados en caso de falla del sistema. Tal como se demostró durante la suspensión de los servicios motivada por el ciberataque, se identificaron diversas formas de atención lo que eventualmente retrasa la atención de asuntos urgentes y eleva los riesgos relacionados con incumplimientos en la atención de disposiciones o comunicados institucionales.

En ese marco se requiere la adopción de acciones que permitan verificar si la suspensión del sistema provocó que no se incluyeran registros de información correspondiente al proceso automatizado, en aras de garantizar la integridad de los datos.

RECOMENDACIONES

LICENCIADA VILMA CAMPOS GÓMEZ, GERENTE A.I, GERENCIA ADMINISTRATIVA O A QUIEN EN SU LUGAR OCUPE EL CARGO

1. Definir y ejecutar en conjunto con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías y la Subárea de Archivo y Correspondencia en el marco de la implementación y funcionamiento del SAYC una estrategia de recuperación de la documentación que respalda la gestión de desarrollo e implementación del Sistema de Archivo y Correspondencia, identificando las causas de su ausencia, así como un plan con las medidas pertinentes para evitar la materialización de situaciones similares a futuro.

   Para acreditar la atención de esta recomendación deberá aportarse la documentación que respalde la estrategia definida, así como los mecanismos de control que garanticen su cumplimiento. Además, se requiere remitir el plan con las medidas para garantizar el respaldo de la documentación generada ante eventuales interrupciones de servicios como la experimentada durante el ciberataque del presente año.

   Plazo de cumplimiento 10 meses a partir del recibo del presente informe.

2. Establecer en conjunto con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías y la Subárea de Archivo y Correspondencia un plan de fortalecimiento de los mecanismos de seguridad en el acceso al SAYC considerando entre otros aspectos la viabilidad de su integración con el Módulo Institucional de Seguridad (MISE), así como la modalidad de doble autenticación.

   Para acreditar el cumplimiento de esta recomendación deberá aportarse la documentación que respalde el plan de fortalecimiento citado, así como los mecanismos de control establecidos para garantizar su cumplimiento.

   Plazo de cumplimiento 10 meses a partir del recibo del presente informe.
3. Definir y ejecutar en conjunto con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías y la Subárea de Archivo y Correspondencia, un plan actualizado

con plazos, responsables y actividades orientadas a la finalización de la implementación del SAYC a nivel institucional, garantizando el uso masivo de esta herramienta al catalogarse ésta como la aplicación oficial para la gestión de asuntos y correspondencia en la CCSS, y considerando la transición requerida en centros de trabajo donde se utiliza actualmente otro mecanismo o herramienta para dicho proceso.

Para acreditar el cumplimiento de la presente recomendación deberá remitirse la documentación que respalde la definición del plan de implementación del SAYC, así como los mecanismos de control definidos para garantizar su cumplimiento.

Plazo de cumplimiento 5 meses a partir del recibo del presente informe.

4. Implementar en conjunto con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías y la Subárea de Archivo y Correspondencia un proceso de revisión sobre la percepción del usuario respecto del SAYC, así como la recopilación y atención progresiva de las dudas, incidentes o propuestas de mejora, lo anterior en aras de mejorar la satisfacción de los funcionarios encargados de la gestión de asuntos y correspondencia en cada unidad institucional donde se utilice dicha herramienta.

   Para acreditar el cumplimiento de la presente recomendación deberá remitirse la documentación que respalde la implementación del proceso de atención a la percepción del usuario SAYC.

   Plazo de cumplimiento 5 meses a partir del recibo del presente informe.

5. Definir en conjunto con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías y la Subárea de Archivo y Correspondencia, un plan de capacitación que considere el fortalecimiento y actualización del conocimiento al personal institucional sobre las funcionalidades del SAYC, considerando revisión y monitoreo periódico, así como concientización sobre el buen uso del sistema y el registro correcto de información.

   Para acreditar el cumplimiento de la presente recomendación deberá remitirse la documentación que respalde el plan de capacitación definido y oficializado.

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

6. Establecer en conjunto con la Subárea de Archivo y Correspondencia un plan con plazos, responsables y actividades orientadas a la definición e implementación del mecanismo de contingencia oficial del SAYC a nivel institucional a fin de garantizar la continuidad de servicios ante eventuales afectaciones en la gestión de asuntos y correspondencia automatizada mediante dicha aplicación informática.

   Para acreditar el cumplimiento de la presente recomendación deberá remitirse el plan para definición e implementación del mecanismo de contingencia oficial del SAYC.

   Plazo de cumplimiento 10 meses a partir del recibo del presente informe.

7. Definir y ejecutar en coordinación con la Subárea de Archivo y Correspondencia una estrategia institucional orientada a completar los registros de datos pertinentes que garanticen la integridad de la información del SAYC de acuerdo con la gestión de asuntos y correspondencia efectuada

durante el periodo de suspensión de ese sistema producto del ciberataque perpetrado el presente año.

Para acreditar el cumplimiento de la presente recomendación deberá remitirse la documentación que respalde la estrategia definida, así como los mecanismos de control establecidos para garantizar su cumplimiento.

Plazo de cumplimiento 6 meses 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 de la Caja Costarricense de Seguro social, los resultados del presente informe fueron comentados el 17 de noviembre del 2022, con los funcionarios de la Gerencia Administrativa Sra. Gabriela Rosales Rosas, asesora de gerencia, Ing. Giorgianella Araya Araya, Directora de Servicios Institucionales, Lic, Gerardo Salazar Gonzalez, Jefe de Área de Publicaciones e Impresos y Licda. Iris Bedoya Cabezas jefe a.i Subárea de Archivo y Correspondencia.

Con relación a los hallazgos expuestos, la administración emitió las siguientes observaciones:

En relación con el hallazgo 1, el Lic. Gerardo Salazar González, consultó respecto a la fecha de implementación de la Metodología de Desarrollo de Software, a efectos de conocer si el sistema fue desarrollado con anterioridad por lo que no le afectaría su aplicación.

Respecto al Hallazgo 2, el Lic. Salazar González informó que al momento de la primera planificación de implementación del sistema se tenían 323 unidades como meta, posteriormente la necesidad de amplió a 600 aproximadamente, lo que afecta la planificación y proyección, no solo los aspectos relacionados con la pandemia y el hackeo.

Sobre el hallazgo 5 el Lic. Salazar González indicó que coincide en que es necesario mejorar el mecanismo de contingencia, cuando se dio el hackeo se vio que no era una solución sostenible, por lo que se desarrolló un nuevo sistema que va a servir como mecanismo de contingencia, donde se va a poder migrar la información una vez que el SAYC sea restablecido. Como experiencia menciona que la contingencia de aplicación es importante, pero una cosa difícil para ellos fue el restablecimiento del sistema, reiniciarlo para más de 500 unidades lo antes posible.

Respecto a los hallazgos 3, 4, 6 y 7 no se emitieron comentarios u observaciones.

Sobre las recomendaciones, se hicieron las siguientes observaciones:

Recomendación 1

Gabriela Rosales Rosas, asesora de Gerencia Administrativa indicó tener dudas, ya que del SAYC comenzaron a ser usuarios a partir del 2014 pero desde antes ya se había elaborado, esta recomendación la dirigiría a la GIT, dado que la gerencia administrativa es la líder del proyecto, pero el producto ya estaba en ejecución desde el 2014 por lo que ya estaba creado y el CGI de la GIT es el responsable de la documentación.

El Lic. Salazar González, agregó que efectivamente para esa fecha ya el sistema tenía un desarrollo importante, además hay 2 herramientas, una versión cliente servidor y una Web, acá estaríamos hablando de la versión cliente servidor que tiene ciertas características y que se está migrando a Web

Esta solicitud fue valorada por esta Auditoría, considerando el rol de dirección en la implementación del SAYC a nivel institucional corresponde a la Gerencia Administrativa de forma tal debe garantizar que se cumpla con la normativa que rige esta materia, además de lo necesario para el éxito del proyecto, en ese sentido, en coordinación con el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías encargado del desarrollo del sistema se valoren las acciones para el cumplimiento de la recomendación. Por lo que a criterio de este Órgano de Fiscalización debe mantenerse tal como se planteó.

Recomendación 2

Gabriela Rosales Rosas indicó que la redacción da a entender que se debe implementar el MISE, pero esto es un aspecto más técnico y no sabe si se debe dirigir a la DTIC o al CGI, se le aclara que ellos son la parte técnica y que lo normal es que sea el dueño del proceso que realice el análisis de cuál es la solución más factible y dependiendo de esto se tomen las decisiones de solicitar la colaboración al CGI o a la DTIC.

Como se indicó en la sesión de trabajo con la administración, se requiere de una valoración del dueño del proceso con la colaboración del ente técnico a efectos de determinar la solución más factible, por lo que este Órgano de Fiscalización mantiene la recomendación tal como se planteó.

Sobre las recomendaciones 3, 4, 5, 6 y 7 no se emitieron comentarios, por lo cual se aceptan los términos establecidos en forma, fondo, plazo y entregables para su atención.

ÁREA DE TECNOLGIAS DE INFORMACIÓN Y COMUNICACIONES

Ing. Alexander Araya Mora
Asistente de Auditoría

Ing. Rafael Ángel Herrera Mora
Jefe

OSC/RJS/RAHM/AAM/jfrc

Anexo 1
Unidades pendientes de implementación SAYC
Agosto 2022

Centro de Salud	Fecha Implementación 2022-2023
Hospital Max Terán Valls Hospital Dr. Rafael Angel Calderón Guardia	Nov (22) – Dic (22) – Ene (23).
Región Huetar Atlántica – Hospitales y Área de Salud - Centro Nacional De Rehabilitación Dr. Humberto Araya Rojas	Ene – Feb – Mar
Región Huetar Chorotega - Hospitales y Área de Salud Hospital San Juan De Dios	Feb – Mar – Abr
Región Huetar Norte - Hospitales y Área de Salud Hospital Nacional De Geriatría Y Gerontología Dr. Raúl Blanco Cervantes	Abr – May – Jun
Región Brunca- Hospitales y Área de Salud Hospital Nacional de Niños Dr. Carlos Saenz Herrera	May – Jun – Jul
Región Central Norte - Hospitales y Área de Salud Hospital De Las Mujeres Dr. Adolfo Carit	Jun – Jul – Ago
Región Central Sur - Hospitales y Área de Salud Hospital Dr. Max Peralta Jimenez	Jul – Ago – Set
Hospital México Hospital Psiquiátrico Manuel Antonio Chapuí Y Torres	Ago – Set – Oct
Áreas de Salud Proveedores Externos	Set- Oct –Nov

Fuente: Oficio DSI-API-0224-2022 del 22 de octubre de 2022, “Informe de implementación del “SAYC” en Centros Médicos