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

ATIC-68-2020
4 de septiembre de 2020

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2020 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de analizar la gestión integral del Proyecto denominado *"Plan de Ciberseguridad para la Caja Costarricense del Seguro Social"*.

Los resultados de la evaluación permitieron establecer oportunidades de mejora en torno a la implementación de los requisitos para el desarrollo de la iniciativa llamada *"IMP15. Establecer Plan Táctico para Ciberseguridad",* entre los cuales se encuentra la *"IMP02. Habilitación del Comité de Riesgos y Seguridad de la Información",* supeditada a la ejecución de la Licitación Pública 2019LN-000001-1150 y que, además, tiene como condición la aprobación de la estructura organizacional de Tecnologías de Información y Comunicaciones por parte de la Junta Directiva.

También, se identificaron aspectos concernientes al cumplimiento del cronograma definido en la fase uno *"Planificación"*, así como su respectiva gestión de cambios. Por otra parte, no se evidenció respaldo documental referente a la justificación del alcance establecido durante la confección del pliego cartelario, la selección de unidades y cantidad de sitios a visitar durante la fase dos *"Situación actual"*, así como la inclusión del equipo médico*, situación que podría impactar en el resultado de las fases posteriores y en la orientación de las diversas iniciativas propuestas por la empresa consultora para el cierre de las brechas.*

Aunado a esto, mediante la revisión de la documentación concerniente al componente de *"Gestión del Cambio Organizacional"*, se evidenciaron aspectos de mejora en torno a la representación de las unidades locales en la red de agentes de cambio definida para el proyecto, lo anterior por cuanto resulta relevante el involucramiento de las personas antes, durante y después de ejecutar una modificación de sus labores contribuyendo con la transición y minimización de riesgos vinculados con la resistencia al cambio y desinformación. Así mismo, se detectaron oportunidades de mejora tendientes a fortalecer el seguimiento y cumplimiento de los acuerdos establecidos durante las sesiones del equipo de trabajo del proyecto.

En virtud de lo expuesto, este Órgano Fiscalizador considera oportuno realizar recomendaciones a la Gerencia General y a la Dirección de Tecnologías de Información y Comunicaciones, con la finalidad de adoptar acciones concretas para poner en práctica las oportunidades de mejora insertas en el presente informe de conformidad con lo establecido en el marco normativo aplicable.

ATIC-68-2020
4 de septiembre de 2020

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES UP: 1150

AUDITORÍA DE CARÁCTER ESPECIAL REFERENTE A LA GESTIÓN INTEGRAL DEL PROYECTO "PLAN DE CIBERSEGURIDAD DE LA CCSS"

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo del 2020 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión integral del Proyecto denominado *"Plan de Ciberseguridad de la CCSS".*

OBJETIVOS ESPECÍFICOS

1. Analizar los requisitos previos a la ejecución de la iniciativa *"IMP15. Establecer el Plan Táctico de Ciberseguridad"* vinculados con el proyecto Modelo de Gobernanza de las TIC y de Seguridad de la Información.

2. Revisar la ejecución contractual de la Licitación Abreviada N° 1019LA-000001-1150 *"Servicios profesionales para el desarrollo del Plan de Ciberseguridad de la CCSS*".

3. Identificar la participación de los niveles organizacionales en la gestión del cambio del proyecto.

4. Comprobar los mecanismos de control ejercidos por la Administración Activa para verificar el cumplimiento de las actividades planificadas.

ALCANCE

El estudio comprende las acciones realizadas por la Dirección de Tecnologías de Información y Comunicaciones, en torno a la gestión integral del proyecto denominado *"Plan de Ciberseguridad de la CCSS"*. Lo anterior considerando el periodo comprendido entre enero 2019 y febrero del 2020, ampliándose en aquellos casos que se resultó pertinente.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Solicitud y revisión del respaldo documental suministrado por la Administración Activa en torno al proceso contractual de la Licitación Abreviada N° 2019LA-000001-1150.
- Aplicación de entrevistas y consultas a los siguientes funcionarios:
  - Ing. Manuel Montillano Vivas, Director del Proyecto "Plan de Ciberseguridad para la CCSS"
  - Alejandra Elizondo Zamora, Encargada del componente denominado Gestión del Cambio Organizacional.

MARCO NORMATIVO

- Ley General de Control Interno, N° 8292.
- Normas de Control Interno para el Sector Público, 2009.
- Normas Técnicas para la Gestión y Control de las Tecnologías de la Información (CGR), 2007.
- Normas Institucionales en TIC, 2012.
- Metodología de Administración de Proyectos (DTIC), 2014.

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 y 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

Las tecnologías de información y comunicaciones se encuentran cada vez más inmersas en las actividades cotidianas de las organizaciones y la Caja Costarricense del Seguro Social, en adelante CCSS, no es la excepción, lo anterior debido a que se han efectuado esfuerzos de automatización en procesos tales como la atención médica de los usuarios en los diferentes centros de salud, la recaudación de las cuotas obrero-patronales, trabajadores voluntarios e independientes a nivel nacional, así como la gestión del régimen de pensiones del sistema de Invalidez Vejez y Muerte (IVM) y el no Contributivo (RNC), entre otros.
En ese mismo orden de ideas, la información transmitida a de un punto a otro mediante la utilización de la red informática debe de ser protegida con prácticas continuas de prevención como por ejemplo la Ciberseguridad, la cual pretende tratar las amenazas relacionadas con el robo de información, sabotaje de la infraestructura y la indisponibilidad de los servicios, utilizando diversas técnicas como Fingerprinting , Ataques día cero , spam y phishing , hijacking , DoS y Rootkits , entre otros.phishing , hijacking , DoS y Rootkits , entre otros.

Proyectos ejecutados por la Institución en relación con la Ciberseguridad

La Caja Costarricense del Seguro Social ha desarrollado proyectos relacionados con la seguridad de la información como, por ejemplo, la Compra Directa N°2014CD-000003-1150 "*Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC",* a cargo de la Subárea de Seguridad Informática, la cual consistió en la contratación de la firma consultora Deloitte & Touche con la finalidad de efectuar el análisis de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones.

Posteriormente, producto de la revisión efectuada por la firma consultora, se determinó una serie de hallazgos concernientes a ingeniería social, equipo médico, red de telefonía, penetración interna y externa, call center, sistema de gestión de seguridad informática, seguridad física, sistemas de información e infraestructura, los cuales se comunicaron mediante informes de evaluación a las diversas unidades interesadas. Además, se confeccionaron planes remediales como mecanismos para mitigar las vulnerabilidades identificadas.

Licitación Abreviada N°2016LA-000003-1150 *"Diseñar e implementar el Modelo de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS"*

Por otra parte, la Dirección de Tecnologías de Información y Comunicaciones, en noviembre de 2016 inició la Licitación Abreviada N°2016LA-000003-1150 "Diseñar e implementar el Modelo de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS", donde se especificó mediante el cartel contractual los siguientes aspectos:

1. Consultoría para el diseño de Modelo de Gobernanza de las TIC.
2. 2.500 horas de Servicios Profesionales por demanda para el desarrollo de actividades aprobadas del Plan de Intervención inmediata generado en la Consultoría para el desarrollo del modelo de Gobernanza de las TIC.

Dicho proyecto tenía como objetivo general diseñar e implementar un modelo meta de Gobierno de TIC y Gobierno de la Seguridad de la información para la institución, mediante la ejecución de siete fases, obteniendo como entregable el plan de acción para el cierre de las brechas identificadas, en el cual se definió la implementación de 36 iniciativas divididas entre las etapas de atención correspondientes a transversales, inmediatas, a corto, mediano y/o largo plazo. Asimismo, se identificaron los productos relacionados con la seguridad de la información, los cuales se muestran en la siguiente tabla:

Tabla N°1
Iniciativas relacionadas con seguridad de la información y su etapa de implementación

Iniciativa	Etapa de implementación
Habilitar la gestión de operaciones de TIC desde la perspectiva de las seguridades operativas.	Corto plazo
Establecer el Plan Táctico de Ciberseguridad	Mediano plazo
Habilitación del Comité de Riesgos y Seguridad de la información	Mediano plazo
Implementar el Sistema de Gestión de Seguridad de la Información	Largo plazo

Fuente: Información recopilada del respaldo documental del Proyecto de Gobernanza de las TIC y de la Seguridad de la información

Por otra parte, el 15 de febrero de 2019, a través del documento 292-2019, la Auditoría Interna en cumplimiento de sus labores de asesoría, efectúa un resumen de los productos emitidos desde el 2014 sobre temas relevantes en torno a la seguridad de la información administrada por la CCSSS, donde se menciona la definición de estrategias para establecer un modelo de gestión integral, el rol de la Dirección de Tecnologías de Información y Comunicaciones, así como sus unidades adscritas referente al fortalecimiento de la infraestructura de seguridad en las TIC.

Así mismo, hace referencia a la importancia de la información dentro de las organizaciones siendo esta uno de los activos más valiosos, así como el insumo para la toma de decisiones en todos los ámbitos, así como la necesidad de establecer un Modelo de Gobierno Institucional para su seguridad, en el cual se gestione de manera eficiente amenazas como lo son el fraude, uso inadecuado, pérdida, robo o corrupción de los datos.

Contratación 2019LA-000001-1150 *"Servicios profesionales para desarrollar el Plan de Ciberseguridad para la CCSS"*

El 22 de enero de 2019, mediante oficio DTIC-0470-2019, el Msc. Manuel Montillano Vivas, funcionario de la Dirección de Tecnologías de Información y Comunicaciones, le indica al Lic. Endry Núñez Salas, Jefe de la Subárea de Gestión de Compras, lo siguiente:

> *"Por medio de la presente, le solicito dar inicio al trámite de contratación para la contratación de "Servicios profesionales para desarrollar Pian de Ciberseguridad para la CCSS". Dicha necesidad está considerada en el plan anual operativo y en el programa anual de contrataciones del año "2019"."*

Además, se adjunta la *"Solicitud de decisión de inicio"*, el cual contiene entre otros aspectos la estimación del monto mínimo de inversión de $520.000.000,00 (Quinientos veinte mil dólares con 0/100) y los entregables solicitados por la Administración Activa divididos en seis fases como se detalla en la siguiente tabla:

Tabla N°2
Entregables definidos en el Plan de Ciberseguridad para la Caja Costarricense del Seguro Social

Fase		Entregable
1.	**Planificación**	• Presentación de sesión de inicio (kick-off), con el equipo de proyecto. • Plan de Proyecto. • Cronograma de proyecto. • Sesión de presentación del entregable de la fase 1 con el equipo de proyecto.
2.	**Análisis Actual**	a. Sesión de presentación y plan de ejecución de la fase 2 al equipo de proyecto de la CAJA. • Informe de Análisis de situación actual de la seguridad en TIC para cada localidad definida en el alcance. • Informe de resultados del análisis de vulnerabilidades técnicas. • Sesión de presentación del entregable de la fase 2 con el equipo de proyecto. • Acta de aceptación de los entregables de la fase 2.

3. Diseño de estado deseado	a. Sesión de presentación del plan de ejecución de la fase 3 al equipo de proyecto de la CAJA • Diseño del plan de Ciberseguridad para la CAJA. • Estrategia de concientización y divulgación del plan. • Sesión de presentación del entregable de la fase 3 al equipo de proyecto. • Acta de aceptación de los entregables de la fase 3.
4. Brechas, riesgos y benchmarking	a. Sesión de presentación y pian de ejecución de la fase 4 al equipo de proyecto. b. Entregable del Plan de Ciberseguridad para la CAJA con las brechas, riesgos de • seguridad en las TIC, y marcos de referencia asociados. • Informe del avance de la gestión el cambio. • Sesión de presentación del entregable de la fase 4 al equipo de proyecto. • Acta de aceptación de los entregables de la fase 4.
5. Hoja de ruta	a. Sesión de presentación y pian de ejecución de la fase 5 al equipo de proyecto de la CAJA. • Entregable de la Hoja de ruta y portafolio inicial de Proyectos de Seguridad en TIC. • Estrategia de revisión y seguimiento de la implementación de los proyectos prioritarios en la hoja de ruta. • Documentar y preparar presentación para de la hoja de ruta y el portafolio de proyectos en ciberseguridad (seguridad informática) al Consejo Tecnológico y Jefaturas correspondientes. • Plan de gestión de cambio de acuerdo con la hoja de ruta. • Sesión de presentación del entregable de la fase 5 al equipo de proyecto de la CAJA. • Acta de aceptación de los entregables de la fase 5.
6. Diseño de mejoras prioritarias	a. Sesión de presentación y pian de ejecución de la fase 6 al equipo de proyecto de la CAJA. • Entregable de los 10 proyectos prioritarios elegidos y documentados. • Sesión de presentación del entregable de la fase 6 al equipo de proyecto. • Acta de aceptación de los entregables de la fase 5.

Fuente: Información suministrada mediante el expediente de contratación Licitación abreviada 2019LA-000001-1150

Como se puede observar en la Tabla N°2, la Administración Activa definió la ejecución del proyecto en seis fases donde se contemplaron aspectos como la planificación del proyecto, el análisis actual de la seguridad en TIC institucional y de vulnerabilidades técnicas, el diseño de estado deseado, la elaboración y entrega del Plan de Ciberseguridad de la Caja, la hoja de ruta, así como el diseño de 10 mejoras prioritarias elegidas y documentadas. Además, se está desarrollando de manera paralela el componente denominado *"Gestión del Cambio Organizacional",* el cual consiste en definir y ejecutar la estrategia de concientización y divulgación del proyecto.

En cuanto al alcance del proyecto, se identificó en el Anexo N°1 del pliego cartelario la descripción de las unidades, infraestructura y servicios de tecnologías de información a visitar durante la ejecución de la fase 2 *"Situación actual"*, las cuales se muestran a continuación:

- Servicios EDUS/ARCA.
- Servicios SICERE.
- Sistema de Pensiones (SIP).
- Esquema de Telecomunicaciones y Video comunicaciones.
- Infraestructura tecnológica y ambientes productivos y no productivos en Oficinas Centrales CAJA y en el Datacenter principal ubicado en CODISA, Hospital San Vicente de Paúl y Gerencia de Pensiones, Hospital

México y Hospital San Juan de Dios. (Léase como infraestructura tecnológica: Telecomunicaciones, Servidores, Sistemas operativos, licenciamiento, equipos de Seguridad, Base de datos, parque tecnológico, entre otros)

- Infraestructura tecnológica de una Dirección Regional de la Gerencia Financiera en la Gran Área Metropolitana.
- Infraestructura tecnológica de una Dirección Regional de la Gerencia Médica y dos áreas de salud dentro de la Gran Área Metropolitana.
- Infraestructura tecnológica y servicios de las TIC de un Centro Hospitalario Nacional de la Gran Área Metropolitana.
- Infraestructura tecnológica y servicios de las TIC de un Centro Hospitalario Especializado de la Gran Área Metropolitana.
- Infraestructura tecnológica y servicios de las TIC de un Centro Hospitalario Regional fuera de la Gran Área Metropolitana.
- Infraestructura tecnológica y servicios de las TIC de un Centro Hospitalario Periférico fuera de la Gran Área Metropolitana.
- Sistema *"Página Web Institucional"*.
- Infraestructura tecnológica de la Gerencia de Pensiones.

El 16 de febrero de 2019, mediante la resolución DTIC-1089-2019, se adjudicó la Licitación Abreviada N° 2019LA-000001-1150 *"Servicios Profesionales para desarrollar el Plan de Ciberseguridad para la CCSS"* a la empresa Price Waterhouse Coopers Consultores S.R.L. y el 19 de marzo de ese mismo año se notificó vía correo electrónico la disponibilidad del contrato N° 010-2019.

Respecto a la ejecución del proyecto con base en el documento confeccionado en agosto del 2019 por parte de la Dirección de Tecnologías de Información *"Informe de avance del Proyecto de Gobernanza y Gestión de las Tecnologías de Información y Comunicaciones en la Caja Costarricense del Seguro Social"*, se indican los siguientes aspectos:

- Para el desarrollo de la fase uno llamada "Planificación", se realizan las primeras reuniones con el equipo de proyecto de la firma consultora Price Waterhouse Coopers (PwC) y se elabora el documento "Plan Proyecto", el cual contiene los objetivos, la descripción de las etapas y el cronograma de actividades, entre otros aspectos.
- En abril de 2019, durante la ejecución de la segunda fase "Situación Actual", se conformó el equipo de trabajo por parte de la Caja con la participación de los siguientes funcionarios:

Tabla N°3
Equipo institucional del Proyecto para el desarrollo del Plan de Ciberseguridad para la CCSS.

Rol	Funcionario(s)
Patrocinador	Robert Picado Mora
Director del Proyecto	Manuel Montillano Vivas
Líder de ciberseguridad	Christian Chacón Rodríguez
Gestión técnica	Ericka Sánchez Solís, Wilfredo Porras Morales, Adrián Madrigal Gómez y Gerardo Chavarría Vargas
Gestión de cambio organizacional	Alejandra Elizondo Zamora

Fuente: Informe de avance del Proyecto de Modelo de Gobernanza y Gestión de las TIC en la CCSS, Dirección de Tecnologías de Información y Comunicaciones.

- Posteriormente, el grupo supra citado con la colaboración de los representantes de la empresa consultora PwC, define las unidades a visitar durante el desarrollo de la fase dos denominada *"Análisis Actual"* de conformidad con los aspectos establecidos en el alcance del pliego cartelario, obteniendo el siguiente resultado:

Tabla N°4
Selección de lugares a visitar durante la ejecución de la Fase dos *"Análisis Actual"*.

Lugar establecido en el alcance	Lugar seleccionado por el Equipo del Proyecto
Dirección Regional de la Gerencia Financiera	Dirección Central de Sucursales – Sucursal de Guadalupe
Dirección Regional de la Gerencia Médica	Dirección Región Central Sur
Área de Salud 1	Clínica Carlos Durán
Área de Salud 2	Cooperativa ASEMECO
Hospital Nacional	Hospital Dr. Rafael Ángel Calderón Guardia
Hospital Especializado	Hospital de Niños Carlos Saénz Herrera
Hospital Periférico	Hospital de Guápiles
Hospital Regional	Hospital Enrique Baltodano Briceño

Fuente: Informe de avance del Proyecto de Modelo de Gobernanza y Gestión de las TIC en la CCSS, Dirección de Tecnologías de Información y Comunicaciones.

- Los equipos del proyecto confeccionaron plantillas con la finalidad de que sirvieran como insumo durante la recolección de información en las entrevistas que se iban a realizar, así como en los lugares a visitar según el alcance contractual y la selección efectuada. Por otra parte, se realizaron sesiones de trabajo con las áreas involucradas en cada uno de los temas de ciberseguridad mencionados en el pliego cartelario.
- Se incorporó paralelamente la ejecución del componente *"Gestión del Cambio Organizacional*", el cual inició con actividades vinculadas con el manejo de expectativas, el diseño del logo, nombre de la iniciativa a desarrollar. Aunado a esto, se trabajó en la organización de la estructura denominada *"Red de Agentes del Cambio"*, la cual hace referencia grupo de apoyo creado para fomentar el compromiso, la aceptación y la participación, impulsando la comunicación bidireccional entre el equipo de proyecto y los colaboradores impactados, alentando el compromiso y la aceptación del cambio, y eliminando la incertidumbre.

Actualmente, según consta en el informe mensual presentado en febrero de 2020, por parte del Director del proyecto al Subgerente de TIC, el proyecto tiene un 51% de avance y se encuentra en el desarrollo de la fase dos, en la cual se han efectuado visitas a los sitios seleccionados de conformidad con el alcance contractual, escaneo de aplicaciones web sin autenticación, reuniones de sensibilización, plan de comunicación a los "*Stakeholders"*[1], la formación y ejecución de la Red de Agentes del Cambio, el proceso de revisión de la información documental, entre otros.

Productos de Auditoría

[1] Persona o grupo que tiene interés en una organización.

La Auditoría Interna como Ente de fiscalización y Asesoría ha elaborado diversos productos relacionados con la seguridad de los datos, los cuales se indican a continuación:

- **ATIC-049-2014:** Evaluación sobre la gestión de la seguridad de la información Institucional y el rol que cumple el área de seguridad y calidad informática señaló la necesidad por parte de la institución para documentar la estrategia y las acciones concretas para implementar un marco que permitiera identificar y clasificar recursos de TI según criticidad. Asimismo, se indicó la relevancia de evaluar los riesgos y generar planes de acción, así como establecer medidas tendientes a la concientización del personal, su capacitación y definición de responsabilidades.

- **ATIC-127-2015**: Estudio sobre el avance en proyectos de adquisición e implementación de software y hardware de seguridad informática, en el cual se evidenciaron oportunidades de mejora relacionadas con el Portafolio Institucional de Proyectos de Inversión en Infraestructura y Tecnologías (PIPIIT) 2014-2018, el cual fue formulado en respuesta de una necesidad de la Caja Costarricense del Seguro Social (CCSS) para definir el rumbo de la institución en los años planteados, también se constató incumplimiento en la planificación en torno a los proyectos referentes a la adquisición de hardware y software de seguridad informática, específicamente en la Implementación CERT institucional y Seguridad en dispositivos móviles BYOD.

- **ATIC-45-2016**: se destacó la necesidad que la CCSS valore la inversión en nuevas herramientas para el fortalecimiento de la seguridad en la plataforma técnica, considerando métricas expuestas por la empresa Gartner en donde se recomienda destinar al menos un 6% del presupuesto total de las organizaciones en ese sentido. Otro aspecto señalado refiere a la suficiencia de recurso humano suficiente y competente en esa materia, así como definición de políticas y normativas actualizadas y alineadas al marco regulatorio establecido por la Contraloría General de la República, y finalmente, la importancia sobre la aplicación de indicadores orientados a alertar oportunamente sobre el límite de accesos a las aplicaciones institucionales, detección de comportamientos irregulares en el uso de sistemas de información y afectaciones al rendimiento de herramientas tecnológicas, entre otros.

- **ATIC-072-2017** Avance en el Proyecto Modelo de Gobernanza de las Tecnologías de Información y Comunicaciones y de la Seguridad de la Información de la CCSS, se evidenciaron oportunidades de mejora relacionadas con la planificación, en aspectos como alcance del proyecto, cumplimiento de cronograma, entre otros, adicionalmente, se determinó la necesidad de disponer de una estimación de costos de la implementación del proyecto que permita a los niveles estratégicos de la Institución, la planificación y priorización de los recursos requeridos para garantizar no solo la sostenibilidad económica del proyecto, sino también el alcance de sus objetivos.

  Además, se evidenció dentro de un marco de proyección para la implementación del modelo meta de Gobierno de TIC y de Seguridad de la Información, la necesidad de definir una estrategia para el aprovechamiento de las 2500 horas contratadas bajo la modalidad de según demanda, en virtud de que deben ejecutarse en un periodo definido. De igual forma, deberá revisarse la participación de personal clave que está involucrado en otros proyectos de alto impacto en la Caja.

  Finalmente, respecto a la administración de proyectos se determinaron debilidades en la gestión de riesgos, documentación de actividades relacionadas con el Modelo Meta de Seguridad de la Información y trámite de pago a la firma consultora, así como otros aspectos de cumplimiento contractual. Por otra parte, se determinaron atrasos en la entrega de los productos; gestión documental no oportuna, aspectos que podrían afectar la consecución de los objetivos planteados en términos del tiempo, alcance y costos.

- **ATIC-106-2017** :este Órgano de Fiscalización recomendó, con el propósito de fortalecer la seguridad informática en la Caja, la integración de un equipo de trabajo para la elaboración de una estrategia de abordaje integral de las vulnerabilidades identificadas en la evaluación ejecutada por la empresa contratada, con el propósito de revisar la aplicabilidad de los planes remediales a los procesos y unidades no incluidos en el alcance de la revisión efectuada, e incorporar las acciones que correspondan producto del análisis mencionado, en los planes estratégicos, tácticos y operativos pertinentes, así como integrar las directrices en la normativa institucional relacionada.

- **ATIC-83-2018** Evaluación de carácter especial referente al cumplimiento de la Ley No. 8968 Protección de la Persona frente al tratamiento de sus datos personales en la CCSS, Se evidenció la ausencia de un modelo de gestión integral orientado al tratamiento y protección de los datos personales administrados por la Institución, además, se carece de un inventario institucional unificado sobre las bases de datos con datos personales, así como una diferenciación de cuales son carácter interno y las que deberían formar parte del ámbito de aplicación de la Ley 8968 y su reglamento por no tener fines exclusivamente internos, personales, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas.

  Por otra parte, se comprobó la necesidad que tiene la Institución de apegarse al concepto de "responsable de base de datos" estipulado en la Ley supra citada, asimismo, existen debilidades en los procesos de inscripción de bases de datos institucionales ante la Prodhab, el establecimiento de medidas de seguridad afines con los términos establecidos en la Ley 8968 y su reglamento, así como el marco normativo institucional vigente en esta materia.

- **Oficio AD-ATIC-26287-2015** Sobre la finalización del ciclo de vida para el soporte técnico del sistema operativo Microsoft Windows Server 2003.

- **Oficio AD-ATIC-56142-2016** Cambio de política de claves en el Directorio Activo (AD) y su posible impacto en la institución

- **Oficio AD-ATIC-60349-2016** Utilidad y funcionamiento del Catálogo Institucional de Aplicaciones informáticas (CIAI)

- **Oficio 47886-2017** Oficio Informativo respecto al marco normativo relacionado con la Privacidad y Confidencialidad de la Información en las Comunicaciones

- **Oficio 53581-2017** "Observaciones relacionadas con la Seguridad Informática de la Información de los servicios institucionales de Tecnologías de Información y Comunicaciones (TIC) accesados a través de dispositivos móviles." Emitido en agosto del 2017 relacionado con la Seguridad Informática de la Información de los servicios institucionales de Tecnologías de Información y Comunicaciones (TIC) accedidos a través de dispositivos móviles, el cual, entre otros, evidenció la ausencia de marco regulatorio que estableciera las directrices y mejores prácticas que a nivel institucional promovieran la seguridad de la información e informática en esos equipos lo cual permitiera a los usuarios reducir los riesgos inherentes a esa tecnología.

  Adicionalmente, en esa misma misiva se señaló la ausencia en la definición de una política de uso, acuerdos de servicio y confidencialidad, que estableciera el ámbito de acción y responsabilidades entre la institución y sus colaboradores a quienes se les brinda autorización para acceder servicios a través de sus dispositivos móviles personales.

- **Oficio 53708-2017** "Aspectos relacionados a la Seguridad Informática de acuerdo con temas abordados en el Convenio de Ciberdelincuencia celebrado en Budapest."

- **Oficio AD-ATIC-5021-2018** Oficio de advertencia sobre la vigencia actual de plataforma tecnológica Institucional y la calidad de la información almacenada en el Sistema Contable Bienes Muebles de la Caja Costarricense de Seguro Social, con énfasis al porcentaje de depreciación en los equipos que conforman la plataforma tecnológica de la Institución, además de analizar un muestreo de los registros del Sistema Contable Bienes Muebles, a fin de verificar la integridad, confiabilidad y oportunidad de los datos.

- **Oficio 6441-2018:** se indicó la necesidad del establecimiento de un Modelo de Gobierno Institucional para la seguridad de la información, a fin de disponer de una visión estratégica en este campo y con ello propiciar un ambiente seguro y controlado que le permita a la CCSS, gestionar de manera eficiente, entre otros temas, amenazas de fraude, uso inadecuado, pérdida, robo o corrupción de información, no sólo en la realización de sus operaciones y funciones, sino también en los servicios que ofrece.

  Además, en ese documento se señaló que la propuesta de Modelo Meta de Gobierno de TIC y Seguridad de la Información no había obtenido las aprobaciones correspondientes, no se presentó en el informe brindado por la Gerencia de Infraestructura y Tecnologías, ni se abordó de manera puntual en la sesión No. 8953 de Junta Directiva del 25 de enero del 2018, a pesar de la importancia que representa el mantener informado a ese Órgano de decisión sobre las estrategias y escenarios para una gestión de riesgos en esa materia con el fin de generar acciones de prevención y mitigación contra actos que afecten la confidencialidad, integridad y disponibilidad de la información.

  También se señaló en ese oficio la falta de comunicación oficial a los gerentes respecto de los hallazgos identificados por la firma PwC en materia de seguridad de la información. En ese sentido conviene mencionar la propuesta del consultor respecto de que la Junta Directiva otorgue aprobación al presupuesto de seguridad de la información, a las políticas, así como al perfil del riesgo asociado (apetito al Riesgo).

- **Oficio AD–ATIC–8137–2018**: Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS donde se valoró la gestión efectuada en el cumplimiento de los planes remediales, producto de la consultoría realizada en la contratación directa 2014CD-000003-1150, “Servicios profesionales para el análisis integral de vulnerabilidades y riesgos en TIC de la CCSS”. En aras de hacer sentido sobre las evaluaciones efectuadas generadas, 1287 hallazgos a los cuales la empresa consultora asignó planes remediales para mitigar los riesgos asociados.

- **Oficio 292-2019:** Oficio sobre aspectos relacionados con la seguridad de la información, en el cual se hace referencia a los diversos productos emitidos por la Auditoría Interna en materia de seguridad de la información y protección de datos personales, mencionando la importancia que reviste la información en las organizaciones, por cuanto se constituye en uno de los activos más valiosos, siendo una de las fuentes principales para toma de decisiones en todos sus ámbitos.

- **Oficio AI-2328-2019:** Oficio sobre la utilización de dispositivos móviles para la prestación de servicios a los usuarios de los regímenes de seguros y pensiones institucionales, con el objetivo de que se realice una valoración de los riesgos asociados a su uso, a efectos de adoptar las acciones necesarias para mantener la información protegida, así como la eficiencia y eficacia en la administración de los recursos institucionales.

HALLAZGOS

1. SOBRE LOS REQUISITOS PREVIOS PARA EL DESARROLLO DE LA INICIATIVA *"PLAN DE CIBERSEGURIDAD PARA LA CCSS"*

De conformidad con la revisión documental referente a las condiciones previas para la ejecución de la iniciativa *"IMP15.Establecer el Plan Táctico de Ciberseguridad"*, se identificó que no se encuentra implementado el prerrequisito *"IMP02. Habilitación del Comité de Riesgos y Seguridad de la información",* el cual a su vez está supeditado a la ejecución de la propuesta *"ITR03. Habilitar la estructura Organizacional de TIC"*, las cuales se encuentran vinculadas de forma integral en el Modelo de Gobernanza de las TIC y de Seguridad de la Información, tal y como se muestra en la siguiente imagen:

Tabla N°5
Prerrequisito de la Iniciativa Plan Táctico de Ciberseguridad

Código: IMP15	**Iniciativa**: Establecer el Plan Táctico de CiberSeguridad	
IDENTIFICACIÓN Y CLASIFICACIÓN		
Perfil	**Tipo**	**Estado actual**
Proyecto	Implementación	Nuevo
Etapa de implementación		
☐ Mejora inmediata ☐ Corto plazo ☑ Mediano plazo ☐ Largo plazo		
Prerrequisitos		
• Comité de Riesgos y Seguridad		

Código: IMP02	**Iniciativa**: Habilitar el Comité de Riesgos y Seguridad de la Información	
IDENTIFICACIÓN Y CLASIFICACIÓN		
Perfil	**Tipo**	**Estado actual**
Acción	Implementación	Nuevo
Etapa de implementación		
☐ Mejora inmediata ☐ Corto plazo ☑ Mediano plazo ☐ Largo plazo		
Prerrequisitos		
• Contar con la aprobación de la Junta Directa sobre el modelo de organización diseñado en el proyecto de Gobernanza de TIC.		

Fuente: Documentación, Modelo de Gobernanza de las TIC y de Seguridad de la Información.

Al respecto, en el documento "*IMP02. Habilitación del Comité de Riesgos y Seguridad de la información"* se estableció como prerrequisito la aprobación del modelo de organización diseñado en el Proyecto de Gobernanza de TIC por parte de la Junta Directiva, por lo cual, el 18 de febrero de 2019, mediante el articulo N°3 de la sesión N°9017, el Máximo Jerarca Institucional acuerda lo siguiente:

> *"ACUERDO TERCERO: se instruye a la Gerencia General y al Proyecto de Restructuración para que analicen la propuesta de Modelo Meta de organización de TIC, el cual forma parte del Modelo Meta de Gobernanza y Gestión de las TIC, y presenten en un plazo de dos meses un informe a la Junta Directiva sobre la propuesta final a considerar."*

En ese mismo orden de ideas, el 13 de febrero de 2020, mediante correo electrónico, la Administración Activa indicó un avance del 94% para la *iniciativa "ITR03: Habilitar la estructura organizacional de TIC", en* virtud de que se encuentra pendiente la aprobación del modelo de organización supra citados por parte de la Junta Directiva.

En vista de lo anterior, se puede constatar más de un año de atraso en la atención del acuerdo supra citado, lo cual materializa riesgos en torno al avance oportuno de implementación del Modelo de Gobernanza de las TIC y de Seguridad de la Información y sus iniciativas asociadas.

Por otra parte, según lo indicado por el Máster Manuel Montillano Vivas, Director del Proyecto, respecto a la propuesta *"IMP02: Habilitar el Comité de Riesgos y Seguridad de la Información",* se evidenció que esta iniciativa no ha iniciado por encontrarse supeditada a la ejecución de la Licitación Pública 2019LN-000001-1150 cuyo objeto es: Servicios profesionales de consultoría para el acompañamiento en la implementación del Modelo de Gobernanza y Gestión de las TIC en la CCSS.

Al respecto, llama la atención de esta Auditoría el desarrollo de iniciativas como la ejecución de la Licitación Abreviada 2019LA-000001-1150 *"Servicios profesionales para desarrollar el Plan de Ciberseguridad para la CCSS",* sin tener implementados los requisitos previos definidos derivadas de Gobernanza, situación que demuestra debilidades en torno al alineamiento entre proyectos que son dirigidos por la misma unidad y se vinculan entre si desde el punto de vista de los procesos de TIC.

La Ley General de Control Interno N°8292, en el artículo 12 *"Deberes del jerarca y los titulares subordinados"*, indica lo siguiente:

> *"En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*
> *a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.*
> *b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades."*

Ese mismo cuerpo normativo en el artículo N°13 *"Ambiente de control",* hacer referencia a lo siguiente:

> *"Ambiente de control. En cuanto al ambiente de control, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:*
> *a) Evaluar el funcionamiento de la estructura organizativa de la institución y tomar las medidas pertinentes para garantizar el cumplimiento de los fines institucionales; todo de conformidad con el ordenamiento jurídico y técnico aplicable.*
> *b) Establecer claramente las relaciones de jerarquía, asignar la autoridad y responsabilidad de los funcionarios y proporcionar los canales adecuados de comunicación, para que los procesos se lleven a cabo; todo de conformidad con el ordenamiento jurídico y técnico aplicable.*

Sobre este asunto, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

> *"A nivel de proyecto de gobernanza se han realizado los esfuerzos necesarios para obtener la aprobación y oficialización de los modelos Modelo Meta y de Organización que requieren las TIC a nivel institucional, sin embargo, en la actualidad dicha decisión está en análisis por las autoridades correspondientes. En esta semana la Gerencia General convocó al Subgerente de TIC y a la*

Directora del Proyecto de Restructuración para analizar la estructura organizacional en tecnologías que más conviene a la organización y una vez se tomé esa decisión, desde el Proyecto de Gobernanza se abordará las diversas iniciativas según la instrucción que se giren de parte del nivel superior.

Por otra parte, a pesar de no tener los prerrequisitos de carácter organizacional y estratégico, el proyecto CIBER TIC continúa, lo anterior dado que en esta fase se está brindando un análisis de la situación actual y las recomendaciones que se emanen serán del ámbito técnico, por lo tanto, se comunicaran en su momento a la estructura organizacional que resulte elegida."

Al respecto, la situación descrita anteriormente resulta relevante por cuanto la propuesta del Modelo de Organización de las TIC fue desarrollado con base en las buenas prácticas como lo es Cobit5, sin embargo, actualmente se encuentra vigente la versión Cobit 2019. Por lo tanto, la institución tendría que invertir en la actualización del respaldo documental asociado a esa iniciativa sin haber implementado la estructura organizacional con la Madurez requerida.

La ejecución de iniciativas sin cumplir con los prerrequisitos establecidos podría ocasionar el desaprovechamiento de los esfuerzos institucionales en materia de TI, lo anterior al implementar soluciones sin tener en cuenta la correlación con proyectos asociados. Además, la ausencia de una estructura organizativa acorde con los resultados obtenidos por la firma consultora propiciaría la materialización de riesgos vinculados con la falta de definición formal del personal a cargo del seguimiento al cierre de las brechas detectadas a través del Plan de Ciberseguridad, lo cual generaría riesgos en torno al desaprovechamiento de los recursos económicos invertidos en temas relacionados con tecnologías de información y comunicaciones.

2. SOBRE EL ALCANCE DEL PROYECTO.

Mediante la revisión efectuada al expediente de contratación 2019LA-000001-1150 *"Servicios profesionales para desarrollar un Plan de Ciberseguridad para la CCSS"*, se identificaron los siguientes aspectos de mejora:

2.1 Sobre el procedimiento utilizado para establecer el alcance del proyecto

Esta Auditoría evidenció la falta de respaldo documental relacionado con los procedimientos que permitieran determinar el tipo de lugares y aplicativos seleccionados en el alcance, así como las unidades y la cantidad de sitios a visitar por nivel de atención durante el desarrollo de la fase N°2 denominada *"Análisis Actual"*. Lo anterior es relevante por cuanto la empresa consultora Price Waterhouse Cooper debe tener el panorama institucional real en temas de ciberseguridad para así efectuar un informe acorde a las expectativas del proyecto, el cual será utilizado como base para la ejecución de las etapas posteriores.

La Ley General de Control Interno N°8292, en el artículo N°15 *"Actividades de Control"*, menciona lo siguiente:

"a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.
b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, lo siguiente:

i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.

ii. La protección y conservación de todos los activos institucionales.
iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente."

Las Normas de Control Interno para el Sector Público, en el Capítulo IV *"Normas sobre actividades de control"*, indican lo siguiente:

> *"Gestión de proyectos*
> *El jerarca y los titulares subordinados, según sus competencias deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes."*

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, establece en el Capítulo 1 *"Normas de aplicación general"*, lo siguiente:

> *"1.5 Gestión de proyectos*
> *La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."*

Al respecto, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

> *"A nivel de cartel se estableció un alcance considerando todo el sistema organizacional de la institución, sin embargo, no existe un procedimiento documental para determinar los lugares ni aplicativos, lo que hicimos fue escoger una muestra de cada uno de los sitios de conformidad con el modelo organizacional institucional, su nivel de criticidad y complejidad tecnológica.*
>
> *A nivel de proyecto, el equipo tuvo la disposición basándose en la experiencia y criterio experto, de crear una herramienta con indicadores que facilitaran la decisión y se ajustara al alcance definido en el pliego cartelario. Esta herramienta presenta los aspectos de selección, el análisis o discusión que se efectuó para seleccionar los sitios no se documentó, lo que se presenta es el resultado final.*"

El no contar con el respaldo documental concerniente a los procedimientos utilizados para justificar el tipo y cantidad de lugares a visitar, así como los aplicativos seleccionados para ser revisados, los cuales sirven para definir el alcance del proyecto y posteriormente, realizar el análisis del contexto actual de la Caja Costarricense del Seguro Social, podría ocasionar un resultado erróneo y por consiguiente, influir en el entregable de la fase dos, lo cual es relevante por cuanto la firma consultora utilizaría esa información como insumo para diseñar el estado deseado, identificar las brechas, riesgos, benchmarking, confeccionar la hoja de ruta con las iniciativas de seguridad en TIC, así como la elaboración y ejecución de las mejoras prioritarias.

Así mismo, llama la atención de este Órgano de Fiscalización y Control no se implementara un método capaz de definir aspectos como la muestra a analizar de conformidad con la cantidad de establecimientos (1043 EBAIS, 107 Áreas de Salud y 29 Hospitales) a nivel nacional durante la fase de marras, para lo cual se debió utilizar un porcentaje representativo que permitiera determinar el nivel de confianza aceptable, así como la certeza del

resultado con insumos estadísticos datos como por ejemplo la revisión del 26% de los EBAIS (281), 78% de las áreas de Salud (84) y un 93% de Hospitales(27), caso contrario a lo identificado en el cartel, donde se visualiza la solicitud de análisis de siete hospitales, dos áreas de salud, dos Direcciones Regionales, y la Gerencia de Pensiones, lo cual determina una un dato inferior a los rangos indicados anteriormente.

2.2 Sobre la inclusión del equipo médico dentro del alcance del proyecto

Se determinó oportunidades de mejora en torno a las muestras establecidas en el alcance del proyecto, lo anterior debido a que no se incluyó el equipo médico en ese apartado, el cual desde un ámbito integral de las TI representan dispositivos con software propietario interconectados a la infraestructura tecnológica institucional, por tanto, también se encuentran sujetos a riesgos de seguridad.

Así mismo, se identificó falta de análisis en la situación actual de estos aparatos tecnológicos durante el desarrollo de la fase 2 *"Análisis actual"*, la cual va a determinar el contexto actual de ciberseguridad en la Caja Costarricense del Seguro Social para posteriormente, diseñar la hoja de ruta a seguir en aras de obtener el modelo deseado y las iniciativas a implementar.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la CGR, en el Capítulo I *"Normas de aplicación general"*, concretamente en el aspecto 1.6 *"Gestión de proyectos"*, indican lo siguiente:

> *"El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización."*

Ese mismo marco normativo, en el Capítulo II *"Planificación y organización"*, específicamente en el punto 2.1 *"Planificación de las tecnologías de información"*, menciona lo siguiente:

> *"2.1 Planificación de las tecnologías de información*
> *La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes."*

Sobre este tema, el Master Manuel Montillano Vivas, Director del Proyecto, indicó lo siguiente:

> *"Como el proyecto es un hijo del Gobernanza, la creación el cartel respetó la plantilla de identificación y clasificación de iniciativas presentadas por la empresa consultora PWC, donde se define el objetivo original, el cual lleva al ámbito táctico y operativo de las gestiones inherentes de la Dirección de Tecnologías de Información y Comunicaciones (TIC), con esto nos enfocamos en nuestro rol institucional, sin embargo, las tecnologías médicas si fueron consignadas en el proyecto, lo anterior por cuanto se hizo la entrega a la empresa de los resultados del estudio de vulnerabilidades efectuado por la Subárea de Seguridad, en el cual se contempló dichas tecnologías en el 2014.*
>
> *Las tecnologías médicas, al no estar dentro de nuestro ámbito de competencia se nos dificulta el asegurar que las recomendaciones emitidas desde el proyecto se cumplan, ya que será responsabilidad de las unidades usuarias de dicha tecnología. Por lo tanto, resulta relevante se*

efectúe una coordinación con el ente rector en el ámbito de las tecnologías de información y el ente rector de las tecnologías médicas."

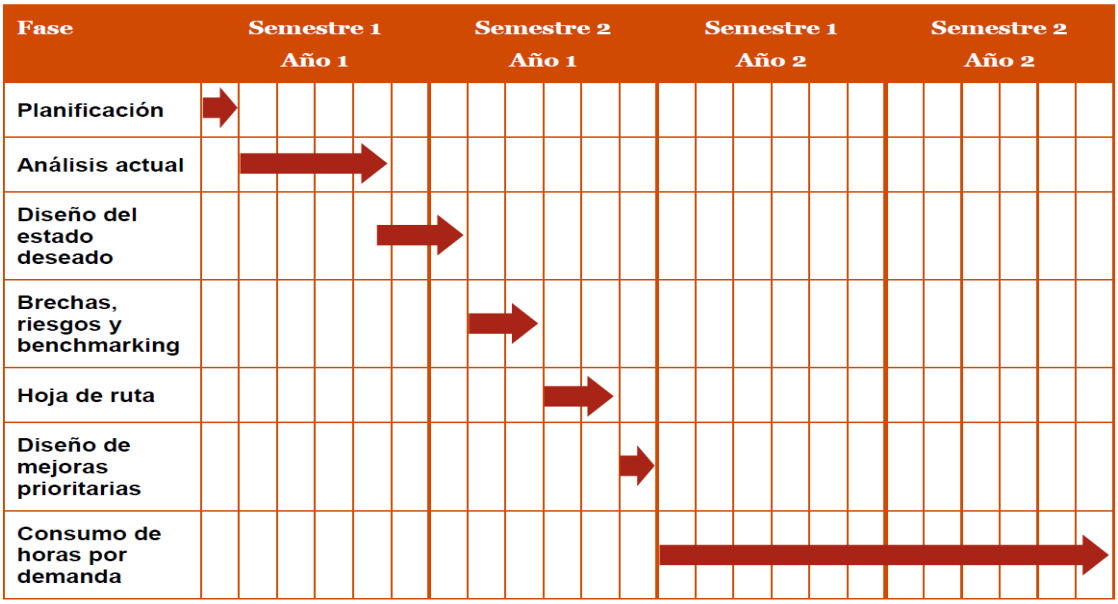
El no contemplar el componente de equipo médico dentro del alcance del proyecto, podría ocasionar que no se visualicen posibles riesgos relacionados con la ciberseguridad de la institución en ese ámbito de acción, limitándole a la empresa consultora la obtención del panorama actual de la institución en ese ámbito y dejando posibles brechas sin identificar durante el desarrollo de la fase dos del proyecto, así como la imposibilidad de incluir mejoras en la hoja de ruta, así como el diseño e implementación de iniciativas en aras de minimizar vulnerabilidades relacionadas con este tema.

3. SOBRE LA PLANIFICACIÓN DEL PROYECTO

3.1 Sobre el cumplimiento del cronograma del proyecto.

Se evidenció un atraso en el cumplimiento de las fechas establecidas en el cronograma de actividades para la ejecución de la Fase dos denominada *"Situación Actual"*, lo anterior debido a que se proyectó una duración de 4 meses para su desarrollo, sin embargo, se contabiliza un total de 11 meses desde su inicio en junio 2019 a mayo de 2020. Por consiguiente, producto de la situación descrita anteriormente, se afectó el tiempo de entrega de las fases tres, cuatro, cinco y seis, así como los plazos del subitem 1.1, por cuanto inicialmente se estableció en el cartel licitatorio y en el documento *"Plan Proyecto"* un término de entrega de 12 meses, tal y como se visualiza a continuación:

Figura N°1
Cronograma resumen del Proyecto para desarrollar el Plan de Ciberseguridad de la CCSS



Fuente: Plan de Proyecto, Price Waterhouse Coopers.

La Metodología de Administración de Proyectos, en el punto 2.4 *"Confeccionar Plan de Proyecto"*, señala lo siguiente:

"La confección del plan del proyecto es uno de los puntos más importantes, ya que este plan es el que permitirá realizar de manera adecuada las siguientes fases del mismo. El objetivo principal de esta actividad es obtener los artefactos que componen el plan del proyecto, que permitan realizar

adecuadamente la ejecución, control y cierre del proyecto. Para lograr esto el líder técnico del proyecto establece y recopila la documentación necesaria para la elaboración del plan del proyecto que posteriormente deberá ser aprobado por la contraparte usuaria."

El pliego cartelario de la Licitación Abreviada N° 2019LA-000001-1150, específicamente en el capítulo *"Condiciones Técnico-Específicas"*, indica lo siguiente:

"3. Plazo de entrega:
Para el sub-item 1.1, el plazo de entrega máximo para todos los productos solicitados es de 12 meses, contados a partir del día siguiente a la notificación de la disponibilidad del retiro del contrato u orden de compra."

Respecto de esta situación, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

"El atraso se debe a varios factores, el primero es que el equipo técnico en la etapa previa a las giras solicitó realizar la revisión de los instrumentos de trabajo efectuando diversos ajustes, los cuales dieron como resultado la extensión del tiempo, provocando un choque con fechas festivas de fin y principio de año y vacaciones de los funcionarios del equipo de proyecto y de los funcionarios a visitar en los sitios seleccionados.

El segundo aspecto hace referencia a los procesos de entrevistas los cuales fueron planificados para aplicarlos a 20 personas, sin embargo, en ciertas sesiones se analizó que era conveniente ampliar el tiempo de estas sesiones e incorporar a otras personas ampliándose a 37 sesiones, como resultado el cronograma del proyecto se actualizo en fechas."

El atraso en la ejecución de las actividades definidas en el cronograma de trabajo podría ocasionar incumplimiento en los tiempos de entrega de las fases posteriores y por consiguiente del proyecto desde la perspectiva integral, la no utilización del presupuesto reservado anualmente por la institución para efectuar el pago de los servicios recibidos, así como la afectación de las actividades cotidianas planificadas para el personal de la Caja Costarricense del Seguro Social posterior a la finalización de la licitación abreviada.

3.2 Sobre la gestión de cambios

Se evidenció oportunidades de mejora en torno a la solicitud, aprobación y documentación de los cambios efectuados al cronograma de trabajo para la ejecución de las seis fases pendientes del proyecto, lo anterior debido a que este instrumento de planificación se ha modificado 5 veces, sin embargo, solamente se evidenció una solicitud formalmente documentada por la empresa Price Waterhouse Coopers correspondiente a la boleta PCS-SCM-001, el 15 de setiembre de 2019, como se indica a continuación:

*"**Razón del cambio***
El cambio que se está solicitando, es causado por razones no contempladas en la planificación inicial del proyecto y que no pueden ser proyectadas por parte de los directores de proyecto, por ejemplo, periodos de vacaciones por dos semanas de los miembros del equipo de proyecto de la CCSS, la situación presentada por la huelga de los empleados de la CCSS y la incapacidad de acordar espacios de agenda de todos los involucrados, por ejemplo.

Detalles del cambio

El cambio consiste en la actualización de las fechas de ejecución de actividades, modificación de actividades de sesiones para la situación actual y adicionar sesiones de trabajo."

La Metodología de Administración de Proyectos, en el apartado 3.4 *"Controlar el Proyecto"*, indica lo siguiente:

"Líder Técnico
Para lograr esto el Líder Técnico del proyecto realiza diversas tareas:
• Recopila las solicitudes de modificación al proyecto y analiza los posibles riesgos involucrados con los cambios solicitados o con ocurrencias sucedidas dentro de la cotidianidad en la ejecución del proyecto, así como el impacto de éstas en el alcance del proyecto con la finalidad de determinar si pueden ser aplicadas o no (…)
Entradas:
2. Solicitudes de Cambios al plan Proyecto. Los mismos se atenderán siguiendo el procedimiento establecido para la Administración de Cambios.
Salidas:
3. Bitácora del Proyecto Actualizada. Consiste en actualizar los documentos de la bitácora del proyecto con las solicitudes de modificación, los informes de avance, directrices administrativas, el plan del proyecto actualizado, el plan de riesgos actualizado y el cronograma actualizado. Modificados por la ejecución del mismo."

Sobre este tema, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

"Solo se cuenta con dos controles de cambio del cronograma oficializados y firmados por los directores de proyecto. Los restantes cronogramas indicados fueron propuestas de las modificaciones que se iban a realizar, por lo tanto, no se tiene respaldo documental relacionado y no se deben considerar dentro del análisis del presente estudio."

Disponer de respaldo documental relacionado con las modificaciones del tiempo de ejecución de actividades durante el desarrollo del proyecto, permitiría efectuar un análisis basado en los hechos que ocasionan las alteraciones, lo anterior con el objetivo de aceptar o rechazar la propuesta realizada, medir el impacto de la actualización respecto de las fechas de cumplimiento para las demás actividades, así como los posibles riesgos involucrados, otorgándole al equipo de trabajo el insumo para poder realizar las acciones necesarias sin alterar el alcance y duración estipulados para la entrega los ítems definidos en el pliego cartelario.

Un proceso adecuado de control de cambios se encuentra orientado a identificar, registrar y fiscalizar las modificaciones presentadas durante la ejecución de un proyecto, proporcionando de manera normalizada, efectiva y eficiente, oportunidades para validar y mejorar el conjunto de actividades que se realizan de manera articulada entre sí, las cuales generalmente tienen como finalidad producir determinados bienes o servicios capaces de satisfacer necesidades o resolver problemas, dentro de los límites de un presupuesto y de un periodo de tiempo dados, por tanto, resulta indispensable documentar los cambios presentados como un mecanismo que permita al equipo de dirección del esfuerzo temporal, comunicar a los interesados de manera sistemática, todas las modificaciones aprobadas y rechazadas en el proyecto y documentar las acciones en aras de identificar oportunidades para proyectos futuros a través de la experiencia adquirida.

4. SOBRE EL COMPONENTE VINCULADO CON EL CAMBIO ORGANIZACIONAL

Se determinó oportunidades de mejora relacionadas con la estructura organizacional del componente denominado "Gestión del Cambio Organizacional", lo anterior por cuanto solo se identifica la participación de funcionarios de 9 hospitales de un total de 29 en la Red de Agentes de Cambio, sin visualizar la representación de personal de Áreas de Salud, Sucursales, Direcciones de Redes Integradas de Prestación de Servicios de Salud, entre otros. Asimismo, es relevante mencionar la función de esta red, la cual es brindar el acompañamiento al personal durante la transición de modificaciones mediante actividades, herramientas y técnicas de tal manera que se logre la aceptación y minimización de riesgos como la desinformación y resistencia a la aceptación de las reformas[2].

La Ley General de Control Interno N°8292, en su artículo N°11 *"El sistema de control interno en la desconcentración de competencias y la contratación de servicios de apoyo"*, indica lo siguiente:

> *"El jerarca y los titulares subordinados tendrán la responsabilidad de analizar las implicaciones en el sistema de control interno, cuando se lleve a cabo una desconcentración de competencias, o bien la contratación de servicios de apoyo con terceros; asimismo, la responsabilidad de tomar las medidas correspondientes para que los controles sean extendidos, modificados y cambiados, cuando resulte necesario."*

Ese mismo cuerpo normativo, en el artículo N° 15 *"Actividades de control"* menciona los siguientes aspectos:

> *"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
> *a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones."*

Aunado a esto, en la ley supra citada, en el artículo *"Valoración del riesgo"*, específicamente en el punto b yd, se hace referencia a lo siguiente:

> *"b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurra y decidir las acciones que se tomarán para administrarlos.*
> *d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar"*

Referente a este tema, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

> *"Inicialmente, se planeó la creación de la red de agentes de cambio solamente con los funcionarios involucrados donde íbamos a realizar las visitas, lo anterior con el objetivo de que ellos tuvieran información sobre el motivo de nuestra visita y se socializara el tema en las diversas unidades.*

[2] Información relacionada con los oficios DTIC-6095-2019, DTIC-5381-2019, DTIC-5382-2019, DTIC-5383-2019, DTIC5384-2019, DTIC-5385-2019, DTIC-5386-2019, DTIC-5387-2019, DTIC-5400-2019, DTIC-5402-2019 ,DTIC-5403-2019, DTIC-0504-2019, DTIC-6098-2019, DTIC-6100-2019, DTIC-6102-2019, DTIC-6103-2019, DTIC-6104-2019, DTIC-6106-2019, DTIC-6135-2019, DTIC-6136-2019,

En vista de lo anterior, no incluimos los diversos funcionarios del ámbito local, debido a que se podía presentar un fenómeno de incertidumbre del alcance del proyecto, por lo tanto, nos enfocamos solamente en los lugares incluidos en el pliego cartelario. Me parece importante el involucramiento por parte de las diferentes áreas de la institución, sin embargo, se tuvieron en cuenta las definidas en el alcance y se estableció una matriz de comunicaciones a nivel de interesados e involucrados.

Además, es relevante indicar, este es el primer proyecto de la Dirección de Tecnologías de Información y Comunicaciones que incluye desde su conceptualización el componente de gestión del cambio organizacional para el desarrollo e implementación del resultado del proyecto, por lo tanto, debemos"

El implementar cambios en las organizaciones requiere la participación, preparación y apoyo de la mayor cantidad de personas antes, durante y después de efectuar las modificaciones, lo anterior con la finalidad de abarcar las diversas unidades involucradas, lo cual puede contribuir en aumentar las probabilidades de éxito del proyecto minimizar la materialización de riesgos vinculados con aspectos como la desinformación y resistencia de los funcionarios cuyas labores se verían impactadas.

5. SOBRE LA GESTIÓN DE MINUTAS

Mediante la revisión documental de las minutas concernientes a la ejecución del Proyecto *"Servicios profesionales para desarrollar un Plan de Ciberseguridad para la CCSS"*, se determinó oportunidades de mejora por cuanto no se visualizó la definición de plazos para la atención de las tareas asignadas a los funcionarios a cargo, así como el seguimiento de las actividades establecidas en sesiones previas del equipo de trabajo que permita a la administración activa llevar un control y verificación del estado de cumplimiento

La Ley General de Control Interno N° 8292, específicamente en el Artículo N° 10 *"Responsabilidad por el Sistema de Control Interno"*, hace referencia a lo siguiente:

"Artículo 10 —Responsabilidad por el sistema de control interno.
Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento."

Las Normas de Control Interno para el Sector Público, en el Capítulo IV *"Normas sobre Actividades de Control"*, establece lo siguiente:

"4.5.2 Gestión de proyectos. El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.

Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:

"(…) c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos

correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.

d. El establecimiento de un sistema de información confiable, oportuna, relevante y competente para dar seguimiento al proyecto…"

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República, en el Capítulo I *"Normas de Aplicación General"*, hace referencia a lo siguiente:

"La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."

Sobre este tema, el Master Manuel Montillano Vivas, Director del Proyecto, indicó en la entrevista efectuada el 24 de febrero de 2020, lo siguiente:

"Tenemos un control de las minutas y una estructura planificada para la definición de los acuerdos, sin embargo, dicha plantillan no cuenta con un cuadro de seguimiento de acuerdos de sesiones anteriores. Adicionalmente los equipos de proyecto efectuamos sesiones semanales donde hablamos de los temas relevantes de la semana y tareas realizar.

Por otra parte, resulta relevante implementar este aspecto de seguimientos y cumplimiento de las actividades pendientes como oportunidades de mejora para llevar mayor control interno por parte del equipo del proyecto CCSS."

Al no efectuar el seguimiento de las actividades asignadas en reuniones previas, así como la falta de establecimiento de fechas para el respectivo cumplimiento, podría ocasionar atrasos en la ejecución de procedimientos posteriores y en las etapas planificadas al momento de su ejecución, así como desconocimiento sobre el tiempo estipulado para brindar seguimiento sobre el cumplimiento de los pendientes por parte de la dirección del proyecto.

CONCLUSIONES

La palabra ciberseguridad se encuentra compuesta por dos estructuras, la primera, ciber del idioma ingles cuya escritura es *"cyber"* y hace referencia a la relación con redes informáticas. La segunda, seguridad del latin *"securitas",* la cual es definida como una cualidad de seguro. En ese sentido podemos concluir que la ciberseguridad es la cualidad de mantener una relación/interacción segura con las redes informáticas al momento de transportar datos, mediante la ejecución de esfuerzos en aras de lograr la protección de la información digitalizada ante amenazas y ataques realizados por personas y/o empresas, cuya intención es provocar daños o favorecerse mediante la extracción de datos confidenciales.

Al respecto, la Caja Costarricense del Seguro Social no está exenta de este tipo de riesgos, por ende, se plantean proyectos con la finalidad de diagnosticar la situación actual y generar acciones para prevenir ataques que provoquen daños a los usuarios de sus servicios y la imagen institucional, tal es el caso de la iniciativa denominada *"Servicios profesionales para desarrollar un Plan de Ciberseguridad para la Caja Costarricense del Seguro Social"*, tramitada mediante la licitación abreviada N° 2019LA-000001-1150, cuyo objetivo general es desarrollar un plan de Ciberseguridad en la CCSS, el cual cuente con los aspectos necesarios para una adecuada estrategia de seguridad de las TIC.

En vista de lo anterior y la importancia que el tema representa dentro de un marco integral de la seguridad de la información, esta Auditoría incluyó su fiscalización en las evaluaciones correspondientes al período 2020.

En primer lugar, los resultados del presente estudio permitieron determinar la necesidad de implementar los requisitos previos a la ejecución de la Iniciativa *"IMP15 Establecer el Plan Táctico de Ciberseguridad*", lo anterior por cuanto el no respetar el orden establecido podría impactar en el logro de un Gobierno de las TIC en la Caja Costarricense del Seguro Social, así como el desaprovechamiento de recursos tanto financieros como humano en proyectos sin tener la estructura organizacional para brindarle continuidad o seguimiento al cumplimiento de los resultados.

En relación con el alcance del proyecto, se evidenciaron elementos a fortalecer referente a los procedimientos utilizados para determinar la muestra de los sitios a visitar y las aplicaciones a revisar durante el desarrollo de la fase N°2 *"Situación actual",* que permitan asegurar una representatividad con el nivel de confianza requerido. Por otra parte, se identificó un atraso en el cumplimiento de las fechas establecidas en el cronograma de actividades para la ejecución de la Fase supra citada, así como la modificación en cinco oportunidades del tiempo de inicio y/o finalización de las distintas fases que lo conforman.

En relación con el componente denominado *"Gestión del Cambio Organizacional",* se determinaron oportunidades de mejora debido a que no se visualizó la representación de funcionarios del nivel local, además, se identificaron aspectos tendientes a fortalecer el sistema de control interno relacionado con el seguimiento de las actividades asignadas para monitorear el cumplimiento de los acuerdos documentados en las minutas correspondientes a las sesiones del equipo de trabajo del proyecto.

En virtud de lo anterior, esta Auditoría propone una serie de recomendaciones a la administración activa, con el fin de solventar los hallazgos identificados, así mismo, resulta pertinente se avoquen esfuerzos de manera integral en aras de lograr el fortalecimiento de la seguridad de la información a nivel institucional, por cuanto este Órgano de Fiscalización ha venido identificando aspectos de mejora a través de diversos productos emitidos desde el 2014, sin visualizar avances significativos respecto a los temas tratados, lo cual es preocupante debido a la posible materialización de riesgos para la CCSS ante la exposición de datos sensibles de la población usuaria de los servicios de salud y pensiones, mediante el robo, uso indebido, fraudes probando implicaciones legales y económicas a la CCSS.

RECOMENDACIONES

AL DOCTOR ROBERTO CERVANTES BARRANTES, EN SU CALIDAD DE GERENTE GENERAL O QUIEN EN SU LUGAR OCUPE EL CARGO.

1. Considerando lo evidenciado en los hallazgos del presente informe, la relevancia de implementar un marco razonable de Ciberseguridad a nivel institucional, así como garantizar la continuidad en etapas posteriores de esta iniciativa, instruir a la Dirección de Tecnologías de Información y Comunicaciones, la elaboración de un plan remedial que valore elementos de gestión y proyecto que han incidido en su avance, lo anterior considerando al menos los siguientes aspectos:

- Iniciativas relacionadas con el Proyecto "Plan de Ciberseguridad" que se encuentran pendientes de formalizar e iniciar según el orden establecido por la firma consultora PWC.
- Las causas que han generado retrasos de los tiempos definidos en el cronograma del proyecto CIBERTIC y lo indicado en el documento *"Plan Proyecto".*

- Lecciones aprendidas que se han presentado en el trascurso del proyecto que permitan prevenir la materialización de posibles riesgos por atraso en las fases posteriores y en los procesos de planificación para futuros proyectos.
- Establecer procesos de rendición de cuentas sobre la gestión efectuada por la DTIC en torno a la implementación de un marco de ciberseguridad institucional.
- Otros elementos que esa Gerencia estime conveniente incorporar.

Posteriormente, la propuesta del plan supra citado se deberá presentar ante la Gerencia General para la respectiva revisión y aprobación. Aunado a esto, esa Gerencia establecerá los mecanismos de monitoreo y control que consideren pertinentes a fin de garantizar su cumplimiento.

Para acreditar el cumplimiento de esta recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de 6 meses, a partir de la recepción del presente informe, el plan remedial formalmente aprobado por esa Gerencia, así como la evidencia documental de las medidas establecidas para garantizar su cumplimiento.

AL MÁSTER ROBERT PICADO MORA, EN SU CALIDAD DE SUBGERENTE DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O QUIEN EN SU LUGAR OCUPE EL CARGO.

2. De conformidad con lo evidenciado en los hallazgos 2.1 y 2.2 del presente informe, efectuar una revisión de los procedimientos utilizados para determinar la definición, justificación y selección del alcance del proyecto, así como una valoración en coordinación con las unidades que se estime pertinente, respecto a la inclusión del equipo médico dentro de esos aspectos, lo anterior con la finalidad de coadyuvar en los resultados de la fase N° 2 *"Situación Actual" e identificar posibles mejoras a incorporar* a partir de una representatividad razonable.

Posteriormente, de ser necesaria la ampliación, realizar las gestiones pertinentes según aspectos legales, administrativos, técnicos, financieros, entre otros. Caso contrario, de no precisar modificaciones, remitir a este Órgano de Fiscalización el respaldo documental que sustente la decisión tomada.

Para acreditar el cumplimiento de esta recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de seis meses, a partir de la recepción del presente informe, el respaldo documental relacionado con los resultados de la revisión y la valoración efectuada, así como las acciones ejecutadas que permitan subsanar lo evidenciado.

3. Con el objetivo de ampliar la representatividad y participación de los niveles locales en la red de agentes de cambio dentro del proyecto, efectuar una valoración que determine la pertinencia de incluir mayor cantidad de funcionarios del ámbito local (Hospitales, Áreas de Salud, Sucursales, Direcciones de Redes Integradas de Prestación de Servicios de Salud, entre otros).

En caso de determinar la pertinencia de incluir personal adicional, realizar las solicitudes formales ante las autoridades correspondientes para su designación dentro del Componente de Gestión de Cambio.

Para acreditar el cumplimiento de esta recomendación, deberá remitirse a esta Auditoría en un plazo de dos meses, a partir de la recepción del presente informe, la documentación efectuada por esa dirección relacionada. con la valoración y las solicitudes formales a las autoridades correspondiente de ser necesario.

4. En virtud de lo evidenciado en el hallazgo cinco del presente informe en torno al seguimiento y verificación del cumplimiento de los acuerdos efectuados a través de las minutas de las sesiones de los equipos de trabajo, valorar la inclusión de controles que permitan monitoreo de las actividades relacionadas con esa temática durante el desarrollo de los proyectos, para lo cual se debe contemplar al menos lo siguiente:

- Acuerdos pendientes
- Descripción
- Responsable
- Plazo de cumplimiento
- Acciones ejecutadas

Para acreditar el cumplimiento de esta recomendación, deberá remitirse a esta Auditoría en un plazo de dos meses, a partir de la recepción del presente informe, la documentación relacionada con la valoración efectuada, así como las acciones ejecutadas que permitan fortalecer el control vinculado al seguimiento y monitoreo de los aspectos mencionados anteriormente.

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 estudio fueron comentados el 17 de julio de 2020 con el Máster Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, el Lic. Juan José Acosta Cedeño, Asesor de la Gerencia General y el Máster Manuel Montillano, funcionario de la Dirección de Tecnologías de Información y Comunicaciones.

A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

Sobre los Hallazgos:

No hay observaciones.

Sobre las Recomendaciones

Recomendación 1:

El Lic. Acosta Cedeño señala que la recomendación es de carácter técnico y los temas mencionados se están abarcando en las demás oportunidades de mejora.

El Máster Picado Mora complementa lo mencionado por el Lic. Acosta Cedeño, haciendo referencia a la relación estrecha que se tiene entre la Gerencia General y Dirección de Tecnologías de Información y Comunicaciones.

En virtud de lo anterior, esta Auditoría concluyó mantener la recomendación uno dirigida a la Gerencia General, por aspectos de objetividad y supervisión jerárquica, efectuando modificaciones de redacción donde esa Gerencia instruya a la Dirección de Tecnologías de Información y Comunicaciones la elaboración de un plan remedial y posteriormente, dicho plan sea presentado para la correspondiente revisión y aprobación, asimismo, se resulta relevante se definan los mecanismos de control y monitoreo que garanticen su cumplimiento.

Recomendación 2:

El Máster Picado Mora solicita se incluya en el segundo párrafo la palabra: técnico.

El Máster Montillano Vivas solicita seis meses para la atención de la recomendación.

En virtud de lo anterior, esta Auditoría Interna concluye incluir las modificaciones solicitadas por el Máster Picado Mora y el Máster Montillano Vivas

Recomendación 3:

No hay observaciones.

Recomendación 4:

No hay observaciones.

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

GRACE MONGE PICADO (FIRMA)
Firmado digitalmente por GRACE MONGE PICADO (FIRMA)
Fecha: 2020.09.04 16:01:06 -06'00'

Ing. Grace Monge Picado
Asistente de Auditoría

ESTEBAN ZAMORA CHAVES (FIRMA)
Firmado digitalmente por ESTEBAN ZAMORA CHAVES (FIRMA)
Fecha: 2020.09.04 16:04:05 -06'00'

Lic. Esteban Zamora Chaves
Asistente de Auditoría

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2020.09.04 16:07:51 -06'00'

Lic. Rafael Ángel Herrera Mora
Jefe Área

RAMH/EZCH/GMP/edvz

Referencia: ID 31304