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

ATIC-106-2017
29-09-2017

RESUMEN EJECUTIVO

Este estudio se realizó en concordancia con el Plan Anual Operativo 2017 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de Información y comunicaciones ejecutado por la Subárea de Seguridad Informática a través de una contratación directa de servicios profesionales con la Firma Consultora Deloitte & Touche.

Los resultados del informe evidenciaron oportunidades de mejora en cuanto a la planificación de actividades requeridas para la ejecución contractual, así como en la definición del alcance de lo contratado.

También se determinó la necesidad de involucrar especialistas y/o responsables de áreas funcionales como por ejemplo, equipo médico, seguridad, física, sistemas de información, pues su participación pudo propiciar una gestión de vulnerabilidades efectiva.

En cuanto al traslado de resultados, se determinaron debilidades ya que se realizó hasta 18 meses después de haber recibido a satisfacción los productos, situación que podría provocar que las acciones para remediar las vulnerabilidades no se efectuaran, pudiéndose materializar los riesgos identificados.

Asimismo, se observó, falta de monitoreo de niveles superiores de la Subárea de Seguridad Informática a cargo del contrato, que pudieron apoyar el desarrollo de la evaluación de vulnerabilidades con una visión integral del tema.

Por otra parte, en relación con la transferencia de conocimiento, la misma no se efectuó conforme lo indicado en el cartel, provocando un desaprovechamiento de este recurso.

Con relación a la ejecución de los planes remediales, el primer seguimiento determinó un cumplimiento de un 15%, de las acciones planteadas por la empresa para los riesgos identificados, por lo que es preciso que la Institución diseñe una estrategia que le permita acreditar que las acciones que mitigan los riesgos y vulnerabilidades se realicen con celeridad y calidad.

En ese mismo sentido, y debido al fin que tienen los planes remediales tal como es la oportunidad de minimizar riesgos identificados en el estudio de vulnerabilidades realizado, su atención e implementación es indispensable para alcanzar este objetivo, por lo que debe brindársele la importancia que representa.

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

Adicionalmente, la Institución hizo una importante inversión económica y de recursos para realizar la contratación, por lo que no otorgarle la atención que merecen los planes remediales propuestos, podría significar un desaprovechamiento de los recursos limitados que dispone la CCSS.

Por otra parte, debido al alcance cubierto por la evaluación realizada, no se analizaron las condiciones de seguridad tecnológica en todos los hospitales, direcciones y demás unidades de la CCSS, situación por la cual es importante que la Gerencia de Infraestructura y Tecnologías, y la Dirección de Tecnologías de Información y Comunicaciones brinden un abordaje integral a las vulnerabilidades encontradas, incluyendo, entre otras acciones, la emisión de políticas que minimicen los riesgos identificados, así como la definición de herramientas y metodologías para analizar en conjunto con funcionarios expertos e instancias que se estime pertinente participar.

Finalmente, la seguridad es un tema sensible a los servicios que presta la institución por lo que es preciso el involucramiento y apoyo de los niveles superiores como patrocinadores de esta gestión.

En virtud de lo expuesto, este Órgano de Fiscalización ha solicitado a la Dirección de Tecnologías de Información y Comunicaciones, a la Gerencia de Infraestructura y Tecnologías, adopten acciones concretas para la atención de las recomendaciones definidas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable.

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

ATIC-106-2017
29-09-2017

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN DE CARÁCTER ESPECIAL REFERENTE A LA GESTIÓN DEL ANÁLISIS INTEGRAL DE VULNERABILIDADES Y RIESGOS DE LA SEGURIDAD EN TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIONES EJECUTADO POR LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES MEDIANTE LA CONTRATACIÓN DE LA FIRMA CONSULTORA DELOITTE & TOUCHE.

GERENCIA INFRAESTRUCTURA U.E. 1107
DIRECCION DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES U.E. 1150

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo del 2017 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de una contratación directa de servicios profesionales a la Firma Consultora Deloitte & Touche.

OBJETIVOS ESPECÍFICOS

- Revisar la planificación y ejecución contractual del proceso de compra 2014CD-000003-1150 “Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC”.
- Verificar la oportunidad en la gestión de la oficialización de los planes remediales establecidos producto del análisis de vulnerabilidades y riesgos en TIC.
- Analizar el cumplimiento de los planes remediales propuestos por la Firma Consultora.
- Revisar la conformación del expediente de la contratación mencionada de acuerdo con lo establecido en la Ley de Contratación Administrativa.

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

ALCANCE

El estudio comprende el análisis de las acciones efectuadas por la Administración Activa en torno a la gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de Información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de la contratación 2014CD-000003-1150 a la firma consultora Deloitte & Touche, en el periodo comprendido entre enero del 2015 al 28 de junio del 2017. La evaluación correspondiente al primer seguimiento entregado por la firma Deloitte, incluyó la versión del 16 de junio de 2017, remitida a esta Auditoría por la Encargada General del Contrato.

La presente evaluación se realizó cumpliendo con las disposiciones establecidas en el Manual de Normas Generales de la Auditoría en el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Revisión y análisis de:

    - Expediente de contratación 2014CD-000003-1150, “Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC”.
    - Documentación suministrada por la Administración Activa referente a la ejecución de la contratación.
    - Entregables por parte de la empresa consultora.

- Entrevistas y reuniones con la Msi. Ana María Castro Molina, Jefe Subárea de Seguridad Informática y Encargada General del Contrato.

MARCO NORMATIVO

- Ley General de Control Interno (No. 8292).
- Ley de Contratación Administrativa y su Reglamento.
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) Nº R-CO-9-2009.
- Normas Técnicas para la Gestión y Control de Tecnologías de Información, Contraloría General de la República.
- Directrices para la Contratación de Servicios de Auditoría Externa en el Sector Público” (D-3-2009-CO-DFOE).

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

ASPECTOS RELACIONADOS CON LA LEY GENERAL DE CONTROL INTERNO

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

La Dirección de Tecnologías de Información y Comunicaciones mediante resolución administrativa, autorizó el 17 de setiembre del 2013, el trámite de Compra Directa 2014CD-000003-1150 referente a servicios profesionales para el análisis integral de vulnerabilidades y riesgos en seguridad de tecnologías de información y comunicaciones (TIC), señalando entre otros aspectos lo siguiente:

> "*A finales del año 2006 y principios del año 2007, se efectuó un estudio de vulnerabilidades integral de la CCSS, y a partir de los resultados de dicho estudio se ha mejorado la infraestructura de tecnologías de información, a la fecha casi siete años después y debido a las mejoras y la evolución de las tecnologías es necesario realizar un nuevo estudio de vulnerabilidades, el cual según las buenas prácticas recomiendan ejecutar con una periodicidad de al menos 2 años, situación que no ha podido implementarse en la institución dadas las limitaciones económicas".*

De acuerdo con la documentación incluida en el expediente de contratación, este procedimiento inició el 16 de mayo del 2014, aplicando para su tramitación el artículo 131, inciso h, del Reglamento a la Ley de Contratación Administrativa por tratarse, a criterio de la Administración, de seguridades calificadas justificando lo siguiente:

> "*En procura de salvaguardar el interés público y para mantener la confidencialidad que este tipo de compras implica, se han tomado las previsiones antes de la contratación, según acciones realizadas en la primera etapa, que implican no exponer información que pueda vulnerar a la institución; durante la segunda etapa en la cual solo brinda información confidencial a la empresa escogida y se firma el acuerdo de confidencialidad, y que se ha acreditado la respectiva razonabilidad de costos*…"

El contrato No. 005-2014, fue firmado entre la CCSS y la empresa Deloitte & Touche, el 9 de junio del 2014, por un monto de $97.350,00 (noventa y siete mil trescientos cincuenta dólares con 00/100).

Según lo indicado en el pliego cartelario, la contratación se promovió para atender en diez fases y dos seguimientos, la evaluación de los siguientes temas:

- Sistema de gestión de la seguridad informática
- Prueba de penetración externa
- Prueba de penetración interna
- Infraestructura tecnológica
- Ingeniería social
- Red de telefonía
- Seguridad Física
- Call Center
- Sistemas de información
- Equipos médicos
- Dos seguimientos a los planes remediales[1] que se propondrían para solucionar las debilidades identificadas.

Mediante oficio TIC-0645-2014 del 18 de junio del 2014, el Ing. Manuel Rodríguez Arce, Subgerente a.i de la Dirección de Tecnologías de Información y Comunicaciones, designó a la Msi. Ana María Castro Molina, Jefe de la Subárea de Seguridad Informática, como Encargada General del Contrato.

Por otra parte, en oficio ASCI-0242-2013, la Msi. Ana María Castro Molina, Jefe a.i de la Subárea Seguridad Informática solicitó el aval al Lic. Leonardo Fernández Mora, Jefe de Subárea de Continuidad de Gestión y al Master Mario Vílchez Moreira, Jefe de la Subárea Aseguramiento de la Calidad, para que los funcionarios que se indican a continuación integraran la Comisión Técnica para la Contratación de Servicios Profesionales para el Análisis de Vulnerabilidades y Riesgos de la Seguridad en Tecnologías de Información y Comunicaciones:

- Ericka Sánchez Solís
- Maikol González Alfaro
- Luis Diego Camacho Barrantes
- Erick Vindas Umaña (Suplente)

[1] Acciones a ejecutar para mitigar los riesgos o vulnerabilidades identificados por la firma Deloitte & Touche.

Adicionalmente, la Msi. Castro Molina indicó en ese mismo oficio que la coordinación de la Comisión estaría a cargo de la Licda. Ericka Sánchez Solís.

La ejecución de la contratación para el análisis de vulnerabilidades y riesgos en seguridad de TIC dio inicio el 19 de junio del 2014.

A continuación, se presentan las oportunidades de mejora identificadas en la gestión del análisis integral de vulnerabilidades y riesgos de seguridad en tecnologías de información y comunicaciones.

HALLAZGOS

1. MODIFICACIÓN DEL ALCANCE CONTRACTUAL

De acuerdo con la revisión efectuada de la documentación aportada vía oficios DTIC-2082-2017, DTIC-2140-2017 y DTIC-3826-2017 dirigidos a la Auditoría Interna, e información entregada digitalmente por la Msi. Ana María Castro Molina, Encargada General del Contrato, y Msc. Ericka Sánchez Solís, funcionaria de la Comisión Técnica, así como la incluida en el expediente de la contratación 2014CD-000003-1150, "Adquisición de Servicios Profesionales para el Análisis de Vulnerabilidades y Riesgos de la Seguridad en TIC"; se evidenció la realización de modificaciones al alcance del objeto contractual ya adjudicado, en dos de las evaluaciones:

- "Evaluación del Call Center": tanto en el cartel como el contrato firmado entre la CCSS y la empresa adjudicada, se había considerado la revisión del centro de contactos de la Gerencia de Pensiones, sin embargo, esta tarea no fue realizada. Asimismo, no consta se haya realizado un análisis de precios sobre el costo de la actividad o grupo de actividades que se dejaron de realizar producto de esta decisión.

- "Evaluación a la Red de Telefonía": en esta fase tampoco se comprobó se efectuara la revisión de la plataforma telefónica de la Gerencia de Pensiones como parte del alcance definido dentro de la evaluación de riesgos y vulnerabilidades, sino que se analizó esa infraestructura en el Hospital México, sin constar en el expediente de ejecución del contrato, el análisis para incluir este nosocomio.

  En ese sentido, no se identificaron documentos donde se analizara el cambio de sitio que se efectuó para la red de telefonía justificando la selección del Hospital México como lugar idóneo para realizar la evaluación de vulnerabilidades. Por otro lado, no se valoró si la dimensión de la red que dejó de revisarse fuera de similar complejidad para efectuar el cambio, sin modificaciones al monto pactado en el contrato.

El artículo 51 del Reglamento a la Ley de Contratación Administrativa (RLCA), indica lo siguiente:

> *"El cartel constituye el reglamento específico de la contratación que se promueve y se entienden incorporadas a su clausulado todas las normas jurídicas y principios constitucionales aplicables al respectivo procedimiento…"*

Sobre el alcance de esta etapa, el cartel y el contrato firmado indican lo siguiente:

> *"(...) en cada call center: Revisión de las Centrales telefónicas, de los servidores principales, de la configuración de la seguridad de las bases de datos, de la configuración del IVR, de configuración de las estaciones de trabajo que se enlazan al call center (conectividad, antivirus, antimalware, filtrado de contenido, antiphishing, cualquier otro software de seguridad que aplique), de la conectividad de los distintos componentes…*"

En cuanto a la evaluación de la red de telefonía, el contrato indicó:

> "*Efectuará la revisión de la configuración, identificación de vulnerabilidades de la red telefónica, el planteamiento de la optimización de la red, Guerra de llamadas en los seguimientos sitios: Oficinas centrales, Gerencia de Pensiones, Hospital San Vicente de Paúl-tecnología VoIP, Area de Salud de Coronado-Analógica…"*

Mediante minuta TI-001-2015 del 23 de abril del 2015, estando presentes la Msi. Ana María Castro Molina, Encargada General del Contrato, el Lic. Daniel Berrocal Zúñiga, funcionario del Centro de Gestión Informática de la Gerencia de Pensiones y la Msc. Ericka Sánchez Solís, funcionaria de la Subárea de Seguridad informática y Coordinadora de la Comisión Técnica, se tomó el siguiente acuerdo:

> "*AC (Ana María Castro) dará respuesta al oficio AGI-151-2015, indicando que por mutuo acuerdo no se contemplará el análisis del Call center de Pensiones dada la inviabilidad de aplicar los cambios que la empresa Deloitte eventualmente indique, como resultado del estudio."*

Con respecto a la modificación del alcance para ambas etapas, el Lic. Eithel Corea Baltodano, Jefe del Área de Gestión Informática de la Gerencia de Pensiones, mediante oficio AGI-151-15 del 20 de abril del 2015, remitió a la Msi. Ana María Castro Molina, Encargada General del contrato, observaciones relacionadas con la plataforma actual de esa infraestructura, indicando lo siguiente:

> *"(…) La solución fue adquirida desde el año 2007 y a la fecha se encuentra obsoleta y desactualizada.*
> - *Esta solución se encuentra sin contrato de Mantenimiento Preventivo y Correctivo.*

- *El proveedor de la solución no ofrece mantenimiento evolutivo...".*

En ese sentido, la Msi Ana María Castro Molina, Encargada General del Contrato, en cuanto a la modificación efectuada indicó:

> *"No se pudo prever la modificación porque al momento de iniciar la contratación las condiciones estaban dadas, en ese sentido, se realizó la coordinación previa durante la elaboración del cartel, sin embargo, durante la ejecución del contrato, dichas condiciones variaron debido al tiempo transcurrido."*

La situación descrita obedeció a debilidades de planificación de la ejecución del análisis de vulnerabilidades y riesgos, en virtud del periodo transcurrido entre la elaboración del pliego cartelario y el momento de llevar a cabo las evaluaciones, debido a que la situación de la Gerencia de Pensiones relacionada con la plataforma de telefonía y Call Center se agravó.

La consideración en el objeto contractual de áreas que posteriormente fueron excluidas durante la ejecución contractual, no permitió que se incluyeran en el estudio otras unidades que sí tenían las condiciones para ser revisadas, provocando un desaprovechamiento de los recursos estimados para el análisis de vulnerabilidades.

Adicionalmente, la situación descrita pudo generar que no se brindara aprovechamiento a los recursos financieros otorgados para la contratación de marras, ya que no fue ejecutada una revisión prevista en el alcance del contrato, siendo que el monto establecido pudo utilizarse en otra evaluación.

2. SOBRE LA PLANIFICACIÓN DE ACTIVIDADES REQUERIDAS PARA LA EJECUCIÓN CONTRACTUAL

Se identificaron oportunidades de mejora en la planificación de actividades requeridas para la correcta ejecución contractual, específicamente en la estimación de recursos y coordinación previa con unidades institucionales objeto de evaluación, lo cual derivó en las siguientes situaciones:

- No se valoró la disposición de tiempo del personal de la CCSS requerido en las distintas evaluaciones contenidas en el alcance, esta situación se evidencia en minutas realizadas por la Comisión Técnica producto de reuniones de seguimiento, así como en el oficio CGIGM-0033-2012 del 18 de febrero del 2013, firmado por el Msc. Esteban Zúñiga Chacón, Jefe del Centro de Gestión Informática de la Gerencia Médica, en el que indica lo siguiente:

  > *"En relación a las tareas que se indican en su oficio, quisiera indicarle que no es factible que las cumplamos tal cual, pues en este momento manejamos prioridades claramente establecidas por nuestro personal es escaso."*

- Se identificó en la minuta de seguimiento No. 2015-0049 suscrita entre la empresa contratada y la CCSS el 5 de junio del 2015, un atraso en el desarrollo de la evaluación de telefonía en el Hospital México, tal como se indica a continuación:

  "(…) CCSS le informa a Deloitte que en Hospital México se podrá ejecutar entre dos semanas la red de telefonía. Deloitte indica que está de acuerdo, y hace la advertencia que este tiempo impactará los tiempos del cronograma"

- No se consideró la criticidad de la evaluación de equipo médico ante la atención de pacientes, lo cual se evidencia en el caso del Hospital Nacional de Niños, mediante oficio SEQM-072-2015, del 30 de enero del 2015, en el cual el Sr. Martín Valverde Corrales, Jefe de la Sección Mantenimiento de Equipo Médico, le informa a la Msi. Ana María Castro Molina, Encargada General del Contrato, lo siguiente:

  "(…) se hace la observación que, por tratarse de equipos médicos disponibles para ser usados, prevalecerá la atención de los pacientes, al momento de hacer la correspondiente revisión, si fuera del caso..."

  En ese mismo sentido, en oficio HSVP-S.A.G.T.E.M-0411-2015 del 19 de junio del 2015, el Ing. Manuel Oporto Mejía, Coordinador de la Subárea de Gestión Tecnológica de Equipo Médico, informó a la Encargada General del Contrato, en lo que corresponde, lo siguiente:

  "Analizada la información enviada por su persona y considerando la cantidad de información requerida se me hace imposible poder suministrarle a la empresa Deloitte & Touche S.A lo requerido; por otro lado considero volver a suministrarles un espacio con cada tecnología que son críticas para la atención de los pacientes se hace muy difícil, ya que la empresa viene en horas donde se tiene que detener la consulta…"

El artículo 1.4 de las Normas de Control Interno para el Sector Público establece que:

"…La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.

En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes:

a. La definición de criterios que brinden una orientación básica para la instauración y el funcionamiento de los componentes orgánicos y funcionales del SCI con las características requeridas. (…)
d. La vigilancia del cumplimiento, la validez y la suficiencia de todos los controles que integran el SCI.
e. La comunicación constante y el seguimiento de los asuntos asignados a los distintos miembros de la
institución, en relación con el diseño, la ejecución y el seguimiento del SCI.
f. Las acciones pertinentes para el fortalecimiento del SCI, en respuesta a las condiciones institucionales y del entorno…"

El artículo 9 de la Ley de Contratación Administración dispone:

"*…Previsión de verificación. Para comenzar el procedimiento de contratación, la Administración deberá acreditar, en el expediente respectivo, que dispone o llegará a disponer, en el momento oportuno, de los recursos humanos y la infraestructura administrativa suficiente para verificar el fiel cumplimiento del objeto de contratación, tanto cuantitativa como cualitativamente*…"

En el artículo 8 del Reglamento a la Ley de Contratación Administrativa (RLCA), inciso f) se señala la obligatoriedad de acreditar en la decisión administrativa que da inicio al procedimiento, lo siguiente:

"(…) Indicación expresa de los recursos humanos y materiales de que dispone o llegará a disponer para verificar la correcta ejecución del contrato…"

Las Normas técnicas para la gestión y el control de las tecnologías de información, indica en el punto 2.2 Administración de recursos financieros lo siguiente:

"*La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable*."

Si bien es cierto, en esta contratación la Administración indicó en el documento de decisión inicial del expediente, disponer los recursos para su ejecución, este Órgano de Fiscalización estima que se establecieron los requeridos en la administración del contrato, sin embargo, no se consideró a lo largo del proceso, aspectos de planificación entre los que se encuentra disponer de personal de diferentes unidades de la Institución para brindar información específica de sus áreas de trabajo, acompañar a los funcionarios de Deloitte & Touche y de la Subárea de Seguridad de Tecnologías de Información a las visitas realizadas, participar en reuniones de trabajo, entre otras gestiones asociadas.

Esta Auditoría estima que la planificación de las actividades y sitios que se iban a evaluar no se realizó con la anticipación requerida, de forma tal que las unidades pudieran tener conocimiento sobre el alcance, su participación y responsabilidades que les correspondía, a fin de que los objetivos se alcanzaran en el tiempo y con la calidad pertinente.

Las situaciones descritas afectaron la oportunidad de entrega de los productos por parte de la empresa contratada, la revisión, traslado de las vulnerabilidades y el plan remedial por parte del Área a cargo del estudio a las unidades correspondientes, lo cual podría provocar la materialización de riesgos que pudieron mitigarse con antelación.

Una inadecuada planificación no garantiza que se brinde la debida atención a las necesidades planteadas por la Institución cuando inició el proceso de contratación administrativa, por lo tanto, no permite alcanzar las metas y objetivos planteados por la Administración.

3. OPORTUNIDAD EN LA GESTIÓN DEL ANÁLISIS DE VULNERABILIDADES

3.1 Oportunidad en la obtención de los productos

Se evidenció que desde la formalización de la resolución administrativa para aprobar y autorizar el trámite de contratación de servicios profesionales para el análisis de vulnerabilidades y riesgos en seguridad de TIC, transcurrieron dos años y ocho meses para la obtención de la totalidad de los productos requeridos por la Administración relacionados con las diez fases o evaluaciones requeridas.

La resolución administrativa que autorizó el trámite se firmó por parte de la Msi. Mayra Ulate Rodríguez, Jefe Área Seguridad y Calidad en TIC y la Máster Laura Blanco Mejía, Subgerente de Tecnologías de Informacion y Comunicaciones, el 17 de setiembre del 2013, haciendo uso de la opción denominada “Objetos que requieren Seguridades Calificadas”, sin embargo, el contrato se formalizó ocho meses después, el 9 de junio del 2014, y el último entregable de los informes de las evaluaciones, generado por la firma consultora se recibió el 18 mayo del 2016.

Las Normas Técnicas para la Gestión y el control de Tecnologías de Información, emitidas por la Contraloría General de la República, indican en el punto 1.2 Gestión de Calidad, lo siguiente:

> *“La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo.”*

Las Directrices para la Contratación de Servicios de Auditoría Externa[2] en el Sector Público" (D-3-2009-CO-DFOE), emitidas por la Contraloría general de la República señalan en el punto 6.6, Plazo de Ejecución, lo siguiente:

> *"La Administración debe establecer un plazo de ejecución de la auditoría externa que sea razonable de acuerdo con los fines de ésta, de manera tal que los servicios sean obtenidos con la oportunidad necesaria para la toma de decisiones y demás acciones atinentes…"*

Dentro de las posibles causas de la situación descrita, se encuentran:

- Dilaciones por parte de la firma contratada en la entrega de al menos cuatro productos de las diez evaluaciones efectuadas, según cronograma previsto, como se muestra en la tabla siguiente:

Tabla 1
Entrega de productos 2014CD-000003-1150

Etapa	Fecha de entrega pactada	Fecha de entrega del producto	Días de atraso
Ingeniería Social	27-03-2015	13-05-2016	288
Equipo Médico	01-05-2015	13-05-2016	266
Red de Telefonía	07-08-2015	18-05-2016	188
Penetración interna	19-03-2015	15-07-2015	18

***Fuente**: Elaboración propia con la información contenida en expediente de ejecución contractual.*

De acuerdo con el cuadro anterior, los productos que presentaron más atrasos se refieren a evaluación de ingeniería social, con 288 días, la de equipo médico con 266 días y la red de telefonía con 188 días.

- Calidad de productos entregados para revisión por parte de la empresa contratista, tal y como lo evidencia la Msi. Ana María Castro Molina, Encargada General del Contrato, en oficio ASCI-0368-2015 del 12 de junio del 2015, dirigido al Señor Luis Guillermo Rodríguez Araya, Socio de la firma Deloitte & Touche, en el cual señala:

[2] Es el servicio brindado por una persona física o jurídica ajena al ente u órgano objeto de estudio, consistente en un proceso sistemático, independiente y profesional para obtener y evaluar objetivamente evidencia, en relación con hechos y eventos de diversa naturaleza; con el propósito de comprobar su grado de correspondencia con un marco de referencia de criterios aplicables; y comunicar los hallazgos o asuntos determinados, así como las observaciones, conclusiones, opiniones, dictámenes y recomendaciones, según corresponda, a la respectiva Administración, con el fin de impulsar mejoras en la gestión, mejorar la responsabilidad pública, promover la calidad de la información contable, financiera y presupuestaria, y facilitar la toma de decisiones. **Tomado del Apartado Glosario de la Directrices para la Contratación de Servicios de Auditoría Externa en el Sector Público" (D-3-2009-CO-DFOE)**

"(…) situaciones que se han venido presentando durante el proceso de contratación, agradeciendo interponga sus buenos oficios a efectos de poder continuar con el proceso y obtener de forma exitosa los productos requeridos a satisfacción de la CCSS, específicamente:

- *Impuntualidad a las sesiones de trabajo tanto de seguimiento como con los sitios locales.*
- *Mal recabo de evidencia que inciden una gestión adicional de coordinaciones con los distintos sitios.*
- *Informes de baja calidad, que han representado revisiones adicionalmente por parte de los funcionarios contraparte de la contratación de la CCSS.*
- *Un alto porcentaje de hallazgos triviales, siendo que existen vulnerabilidades importantes de ser evidenciadas como parte del alcance del presente estudio.*
- *En el caso de la etapa de ingeniería social, por el alcance fue posible avalar dar una nueva oportunidad para re-ejecutar, sin embargo, tenemos una situación de no satisfacción del producto, en la etapa de equipo médico…"*

- Múltiples revisiones y devoluciones por parte de la Comisión Técnica y de la Encargada General del contrato, de los documentos aportados por la firma consultora, aspecto que se constató en las minutas de las sesiones de trabajo efectuadas y lo expuesto por la Msi. Castro Molina en el oficio citado supra.

Se evidenció el cobro de multas realizado por la Administración, a la firma Deloitte & Touche, por los atrasos presentados durante la ejecución de al menos siete de las diez fases evaluadas, siendo que la firma, según indicó la Licda. Ana María Castro Molina, Encargada General del Contrato, debió cancelar a la Institución, por este concepto, $13.142,00 (Trece mil ciento cuarenta y dos dólares con 00/100).

No disponer de los resultados de las evaluaciones solicitadas en el pliego cartelario en los tiempos estimados por la misma Administración puede generar que las vulnerabilidades presentes en cada tipo de evaluación, se materialicen o que no se brinde la atención a las acciones que pudieran mitigarlas exponiendo a la Institución a riesgos en la prestación de sus servicios, tanto en su continuidad como en la calidad

3.2 Sobre la oportunidad en la comunicación de los hallazgos y planes remediales

Se determinó que el traslado formal de los hallazgos y sus respectivos planes remediales por parte de la Encargada General del Contrato a las Unidades que debían atenderlos, no fue realizado de forma oportuna ya que se identificaron plazos extendidos entre las fechas en que fue entregado el documento del informe de cada evaluación por la firma consultora y aceptado por la Institución, y la que se remitió a la instancia correspondiente, tal y como se especifica en la siguiente tabla:

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

Tabla 2
Fechas de remisión de los informes de evaluación por etapa

Fases o Etapas	Fecha acta aceptación definitiva	Fecha de comunicación de los hallazgos
Ingeniería Social	13/05/2016	24/06/2016 Presidencia Ejecutiva
Equipo Médico	13/05/2016	30-05-2016 Hospital San Vicente de Paúl 09/06/2016 Hospital Nacional de Niños 24/06/2016 Hospital San Juan de Dios
Red de telefonía	18/05-2016	30/05/2016 Hospital San Vicente de Paul 09/06/2016 Hospital Nacional de Niños 20/06/2016 Área de Salud de Cartago 27/06/2016 Hospital México
Penetración interna	26/10/2015	Producto de la Subárea, no hubo traslado.
Call center	09/07/2015	14/01/2016 Dirección de Cobros
Sistema de gestión de seguridad informática	09/12/2014	Producto de la Subárea, no hubo traslado.
Seguridad física	09/12/2014	30/05/2016 Hospital San Vicente de Paul 09/06/2016 Hospital Nacional de Niños 20/06/2016 Área de Salud de Cartago 24/06/2016 Hospital San Juan de Dios
Sistemas de Información	25/08/2015	18/01/2016 Área ingeniería de sistemas 12/02/2016 Gerencia de Pensiones 29/02/2016 Gerencia Administrativa 30/05/2016 Hospital San Vicente de Paúl 09/06/2016 Hospital Nacional de Niños 22/01/016 CGI Gerencia de Infraestructura y Tecnología 23/06/2016 Clínica Dr. Carlos Durán
Evaluación Infraestructura tecnológica	24/08/2015	22/01/2016 (Monseñor Sanabria)
		14/01/2016 (Área de comunicaciones y Redes)
		14/01/2016 (Área de Soporte técnico
Penetración externa	09/12/2014	Producto propio de la Subárea, no hubo traslado
Primer Seguimiento	Con prórroga otorgada al 31 03-2017	16/06/2017

Fuente: *Elaboración propia con la información contenida en expediente de ejecución contractual*

Llama la atención los plazos de remisión de los documentos de identificación de vulnerabilidades obtenidos producto de las evaluaciones aplicadas a Infraestructura Tecnológica, Seguridad física, Call Center de Cobros y sistemas de información, para su atención por parte de las unidades instituciones correspondientes, ya que tardaron alrededor de cuatro, diecisiete, seis y cinco meses respectivamente desde que fueron recibidos a satisfacción por la Comisión Técnica a cargo.

La Ley General de Control Interno, en su artículo 12, Deberes del Jerarca y de los titulares subordinados en el sistema de control interno, en los puntos a) y b) señala:

> *"En materia de control interno, al jerarca y a 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 acciones correctivas, ante cualquier evidencia de desviaciones o irregularidades…"*

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el punto 1.3, relacionado con la gestión de riesgos, señalan:

> *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."*

Sobre esta situación, se le consultó a la Msi. Ana María Castro Molina, Encargada General del Contrato, quien indicó lo siguiente:

> *"Primero se presentó limitaciones en el recurso humano para hacer el traslado de información, por otra parte, se dio una priorización de temas por atender por parte de la jefatura del ASCI, asimismo, se buscó darle un abordaje integral al traslado de la información a los encargados.*
>
> *Por otra parte, la ejecución del primer seguimiento se iba a realizar una vez terminadas la totalidad de las etapas de la revisión de los componentes de TIC."*

Lo anterior, podría comprometer la continuidad de los servicios institucionales, debido a la comunicación tardía de las vulnerabilidades y de las acciones de mejora para mitigarlas, por parte de la Encargada General del Contrato, impactando negativamente en la ejecución oportuna de los planes remediales para subsanar los riesgos identificados. La falta de oportunidad en la remisión de los documentos mencionados no propicia un ambiente de seguridad en la Caja, debido a que no hay una respuesta

adecuada a las amenazas, lo cual genera no solo ineficiencia en la gestión de la administración, sino que también aumenta el nivel de exposición al riesgo de las unidades.

4. SOBRE EL INVOLUCRAMIENTO DE PERSONAL ESPECIALIZADO EN LA GESTIÓN DEL ANÁLISIS DE VULNERABILIDADES Y RIESGOS

Se determinó que en al menos seis etapas de las diez realizadas en el estudio de vulnerabilidades, no se involucró en actividades relativas al desarrollo del estudio, aceptación de los productos, comentario de resultados y análisis de vulnerabilidades encontradas; a funcionarios especialistas y/o con las competencias técnicas en el campo de la evaluación con el fin de validar lo indicado por la firma consultora y apoyar los criterios institucionales utilizados en la ejecución contractual. Tal es el caso de las evaluaciones de:

- Infraestructura tecnológica
- Red de telefonía
- Evaluación física
- Call Center
- Sistemas de información
- Equipos médicos

Es importante mencionar que en ese sentido particularmente la Dirección de Tecnologías de Información y Comunicaciones dispone en su organización de áreas especializadas en los temas objeto de las evaluaciones, a saber, ingeniería de sistemas, telefonía IP e infraestructura tecnológica. Asimismo, en la Gerencia de Infraestructura y Tecnologías se ubica la Dirección de Equipamiento Institucional con especialidad en equipos médicos.

Por otro lado, en las actas de aceptación consta que los entregables elaborados por la firma consultora fueron recibidos únicamente por funcionarios de la Comisión Técnica, de la Subárea Seguridad en Tecnologías de Información, a saber, la Msi Ana María Castro Molina, la Msc. Ericka Sánchez Solís, así como el Lic. Diego Camacho Barrantes de la Subárea de Calidad, sin que conste el apoyo de personal adicional especializado en los temas abordados, el cual analizara la existencia y pertinencia de las vulnerabilidades y riesgos identificados, así como la factibilidad de implementar las acciones propuestas, según la realidad institucional, y apoyara la fundamentación de la decisión de recibir a conformidad los documentos de informes presentados por Deloitte & Touche.

En cuanto al comentario de los resultados de las evaluaciones, no se evidenció reuniones en las cuales se analizarán los hallazgos y sus planes remediales, únicamente se identificaron reuniones de presentación de los mismos.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, indica con respecto a las decisiones sobre asuntos estratégicos en el punto 1.6 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."*

Las Directrices para la Contratación de Servicios de Auditoría Externa en el Sector Público" (D-3-2009-CO-DFOE), emitidas por la contraloría General de la República, señalan en el punto 7. Control de la Ejecución del contrato, lo siguiente:

> "*La Administración debe establecer medidas de control sobre la ejecución de la contratación de los servicios de la auditoría externa, que le permitan asegurar que esos servicios cumplen los estándares de calidad definidos y las condiciones contractuales pactadas. Para ello debe designar la unidad o funcionario con competencia y conocimientos necesarios, que fungirá como contraparte de la contratación de los servicios de auditoría externa y, en tal condición, tendrá la responsabilidad de velar por el debido cumplimiento de la contratación y de recibir a satisfacción el servicio pactado."*

En ese sentido, se le consultó a la Msi Castro Molina si se comentaron los hallazgos con los encargados de las Unidades que debían atenderlos para su validación, de previa a la entrega formal, indicando lo siguiente:

> *"No se validaron o comentaron porque la metodología era de Caja negra lo cual implica una revisión de la fase, identificación de los hallazgos, revisión por parte de la Subárea y las devoluciones correspondiente. Luego se transfieren al usuario responsable del tema para la aplicación de las mejoras."*

Sobre el involucramiento de otros funcionarios para facilitar el proceso y los entregables para cada etapa, la Msi. Ana María Castro Molina, Encargada General del Contrato, indicó:

> "*Como encargado definido no había, pero si habían responsables de entregar la información según el ámbito de competencia de cada producto o etapa a la empresa consultora. A ellos mismos se les entregaron los resultados. Dependiendo del producto de la etapa, se le solicitó información de previo a diferentes áreas, como por ejemplo para sistemas de información se solicitó a los CGI´s, información de los sistemas a su cargo*."

El no considerar personal con las competencias técnicas y funcionales en la realización del estudio, en áreas determinadas pudo haber ocasionado que no se hayan identificado vulnerabilidades existentes o que se determinaran riesgos que no reflejen la realidad de la Institución. Adicionalmente, la situación descrita provocó que se identificaran vulnerabilidades que no correspondían a determinadas unidades, o que fueran remitidas a las que no tuvieran competencia para atenderlas.

La situación descrita en el presente hallazgo no propició que se brindara una conducción a la firma contratada con un enfoque de eficiencia que permitiera aprovechar la experiencia y especialidad de la empresa seleccionada como idónea por la misma Administración, pudiendo generar un desaprovechamiento de los recursos disponibles para la ejecución del análisis de vulnerabilidades y riesgos en seguridad de TIC.

5. SOBRE EL ANÁLISIS DE PREVIO A LA REMISIÓN DE PLANES REMEDIALES

Se determinó la ausencia de análisis previo sobre las competencias requeridas para la designación de responsables en la atención de las acciones propuestas, tampoco se evidenciaron acciones de planificación para brindar un abordaje integral para el cumplimiento de los planes remediales sobre vulnerabilidades similares para diferentes unidades evaluadas, lo cual derivó en las siguientes situaciones:

- Se apreció en la evaluación de la seguridad física, la propuesta de aproximadamente 185 acciones a ejecutar producto de los planes remediales, las cuales corresponden a mitigación de riesgos similares identificados en once unidades evaluadas, tal y como se muestra a continuación:

Tabla 3
Unidades evaluadas seguridad Física

Unidades evaluadas	Acciones plan remedial
Área de Salud de Cartago	19
Call Center de cobros	8
Edificio Da Vinci	18
Edificio Laureano Echandi	18
Edificio Jenaro Valverde	14
Hospital México	14
Hospital de Niños	9
Hospital Monseñor Sanabria	25
Hospital Rafael Angel Calderón Guardia	20
Hospital San Juan de Dios	22
Hospital San Vicente de Paul	6
TOTAL	**185**

***Fuente**: Elaboración propia con la información contenida en expediente de ejecución contractual*

- En oficio AIS-0053-2016-N, del 15 de febrero del 2016, emitida por el Master Danilo Hernández Monge, Jefe del Área Ingeniería de Sistemas, señaló que al menos 21 de las acciones y riesgos no le correspondían a su Unidad.

- El Máster Hernández Monge, en ese mismo oficio señaló lo siguiente:

  "(…) *el Módulo de cobros SICERE es parte integral del Sistema Centralizado de Recaudación (SICERE), el cual se encuentra registrado con el número de activo 845355. Por lo tanto la vulnerabilidad indicada no existe."*

- Mediante oficio DCO-0385-2016 del 26 de abril del 2016, el Lic. Luis Diego Calderón Villalobos, Director de Cobros, le señala al Lic. Robert Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones, aspectos relacionados con el oficio ASCI-0027-2016 del 14 de enero del 2016, indicando lo siguiente:

  "Mediante oficio ASCI-0027, de fecha 14 de enero de 2016, la licenciada Ana María Castro Molina, Jefe del Área Seguridad y Calidad Informática, remite a esta Dirección, los hallazgos encontrados en la Evaluación realizada al Centro de Llamadas de la Dirección de Cobros, relacionado con la contratación 2014CD-000003-1150"Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en Tecnologías de Información y Comunicaciones en la CCSS". Analizado dicho oficio se determinó que para la atención de ciertos hallazgos se requiere de la intervención de las diferentes áreas y subáreas de la Dirección de Tecnologías de Información (DTIC)."

Las Directrices para la Contratación de Servicios de Auditoría Externa en el Sector Público" (D-3-2009-CO-DFOE) emitida por la Contraloría General de la República, indica sobre el control de la ejecución del contrato, lo siguiente:

"*La Administración debe establecer medidas de control sobre la ejecución de la contratación de los servicios de la auditoría externa, que le permitan asegurar que esos servicios cumplen los estándares de calidad definidos y las condiciones contractuales pactadas. Para ello debe designar la unidad o funcionario con competencia y conocimientos necesarios, que fungirá como contraparte de la contratación de los servicios de auditoría externa y, en tal condición, tendrá la responsabilidad de velar por el debido cumplimiento de la contratación y de recibir a satisfacción el servicio pactado*."

Asimismo, la Msi. Castro Molina, señaló sobre el análisis previo a la remisión de los hallazgos, lo siguiente:

"No se realizó un análisis previo a la remisión de los hallazgos para determinar la forma en que se iban a gestionar, la entrega se hizo de acuerdo con lo establecido en el cartel de la contratación y se agrupó según los sitios involucrados en cada una de las evaluaciones.

Por otra parte, por un asunto de economía y gestión de recursos, se agrupó la entrega de las oportunidades de mejora de todas las etapas para realizar una única visita al sitio."

La omisión de un abordaje integral a las vulnerabilidades identificadas, no propició tener una visión completa de la situación institucional que permitiera diseñar un plan o estrategia para atender riesgos similares que afectaran a toda la Institución. De igual manera, no fue posible orientar y apoyar en la atención de las acciones a las unidades a las que se trasladaron los planes remediales.

La situación descrita también ocasionó que no fueron trasladadas oportunamente para su atención, las acciones de mejora a las vulnerabilidades encontradas, a las Unidades que debían atenderlas, posibilitando que no se realizaran o que no fueran dirigidas al área competente. Adicionalmente, esa falta de oportunidad podría ocasionar que los riesgos se materialicen, afectando la continuidad y eficiencia de los servicios que presta la Caja.

Asimismo, la remisión incorrecta de planes remediales a unidades sin competencia para su atención, provocó que se dieran por inaplicables, causando que los riesgos identificados por la firma a cargo del estudio no hayan sido mitigados con la celeridad requerida por la Unidad que sí tenía la competencia.

6. SOBRE EL CRITERIO DE SELECCIÓN DE LAS UNIDADES Y EQUIPOS EVALUADOS Y SU REPRESENTATIVIDAD EN LA INSTITUCIÓN.

No consta en el expediente de la contratación, los criterios utilizados para la selección de las unidades y áreas de trabajo institucionales objeto de la evaluación de vulnerabilidades y riesgos en seguridad de TIC. Asimismo, la cantidad de sitios y equipos revisados no representan una muestra significativa de los que dispone la Institución. En la siguiente tabla se muestra los sitios evaluados para cada una de las etapas:

Tabla 4
Sitios evaluados por Etapa

Etapas	Sitios evaluados	Observaciones
Pruebas de Penetración Externa	Oficinas centrales Data Center Gerencia de Pensiones Hospital México Hospital San Vicente de Paúl	5 localidades

Etapas	Sitios evaluados	Observaciones
Evaluación Penetración Interna	Oficinas Centrales (dos edificios) Data Center de la CCSS Hospital Dr. Rafael Angel Calderón Guardia.	5 localidades
Evaluación de equipos médicos	Hospital San Juan de Dios Hospital San Vicente de Paúl Hospital Nacional de Niños	10 equipos por hospital
Evaluación de Call Center	Direccion de Cobros	1 Call Center
Evaluación Red de Telefonía	Oficinas centrales Hospital México Hospital San Vicente de Paúl Area de Salud de Cartago	4 Unidades
Evaluación Sistemas de Información	Gerencia de Pensiones	6 sistemas
	Gerencia de Infraestructura	1 sistema
	Gerencia Administrativa	5 sistemas
	Gerencia Financiera	15 sistemas
	Gerencia Médica	2 sistemas
	Gerencia de Logística	1 sistema
Evaluación Física	Área de Salud de Cartago Call Center de cobros Call center pensiones Edificio Da Vinci Edificio Laureano Echandi Edificio Jenaro Valverde Hospital México Hospital de Niños Hospital Monseñor Sanabria Hospital Rafael Angel Calderón Guardia Hospital San Juan de Dios Hospital San Vicente de Paul	12 localidades

Fuente: *Informe de primer seguimiento Deloitte & Touche*

Lo anterior, se evidencia en los siguientes aspectos identificados:

- Para la evaluación de equipos médicos se seleccionaron tres hospitales, a saber Hospital San Juan de Dios (Hospital Nacional), Hospital Nacional de Niños (Especializado) y el Hospital San Vicente de Paúl (Hospital Regional), lo que corresponde a un 10.35% de los 29 nosocomios que dispone la CCSS.

- En relación con el equipo médico evaluado, se revisaron 30 dispositivos en total, es decir, 10 por cada hospital mencionado anteriormente. Si bien es cierto esta cifra podría no ser representativa con respecto a la totalidad de equipamiento de esta índole, se debe indicar adicionalmente que no consta documentación en la cual se refleje el análisis realizado para identificar y seleccionar la cantidad de equipos susceptibles de valoración, considerando su complejidad.

- Para la revisión de la red de telefonía se revisó únicamente un área de salud, que con respecto a los más de 100 establecidos en la Institución, representa menos de un 1%.

La Ley General de Control Interno, señala en el artículo 14, sobre la valoración del riesgo lo siguiente:

> "*En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros los siguientes:*
>
> *a) Identificar y Analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales…"*

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el punto 1.1 relacionado con la gestión de calidad, señalan:

> *"La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo."*

En ese sentido, la Encargada General del Contrato, Msi Castro Molina indicó:

> "*Para seleccionar la muestra de unidades a evaluar se utilizó el criterio experto del equipo de trabajo a partir de la revisión de las unidades que cumplían con los requerimientos de la evaluación, por ejemplo, a nivel de equipo médico se seleccionaron: un hospital Nacional, un hospital regional y un Hospital especializado, dado que son los que cuentan con equipo médico especializado.*
>
> *En el tema de Call Center, las únicas dos unidades al momento de ejecución del cartel con dichos servicios, eran la Gerencia de Pensiones y la Dirección de Cobros.*
>
> *Por su parte, para el estudio de penetración, se seleccionó a la Gerencia de Pensiones por las recomendaciones de las Auditorías Interna y Externa (Carvajal & Colegiados).*
>
> *Finalmente, en cuanto a la representatividad de la muestra, por un criterio de costos.*

En cuanto a equipos médicos se solicitó un inventario donde se identificaran dichos equipos y se seleccionaron 10 de cada hospital, para tratar de dar cobertura a la máxima cantidad de tipos de equipos médicos".

La falta de criterios para priorizar y seleccionar los sitios y equipos médicos donde se realizarían las evaluaciones podría ocasionar que se revisen vulnerabilidades a unidades y dispositivos médicos con exposición al riesgo con menor probabilidad de ocurrencia y/o impacto, dejando de evaluar los que presenten una calificación mayor, provocando que se puedan materializar riesgos no identificados ni gestionados por la Administración.

La cantidad y representatividad de los sitios y equipos médicos seleccionados para las evaluaciones podría dificultar tener una visión integral de los riesgos y vulnerabilidades a que está expuesta la Institución provocando que no disponga de planes integrales para atenderlos, en detrimento de la prestación de servicios de salud y de pensiones que se brindan tanto en centros de salud, sucursales como el resto de oficinas de la Institución.

7. SOBRE LA CONSIDERACIÓN DE ASPECTOS A EVALUAR EN LA PRUEBA DE PENETRACIÓN EXTERNA.

No se evidenció que en el pliego cartelario, se haya considerado en la evaluación de penetración externa de los sitios seleccionados por la Administración, la revisión de enlaces alámbricos e inalámbricos, acceso a bases de datos y sistemas de información, entre otros, aspectos que podrían afectar la seguridad física y lógica de la información institucional.

Las Normas Técnicas para la Gestión y Control de Tecnologías de Información, emitidas por la Contraloría General de la República, en cuanto a la seguridad física y ambiental, punto 1.4.3, establecen:

"*La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.*

Como parte de esa protección debe considerar:

a. *Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.*
b. *La ubicación física segura de los recursos de TI.*
c. *El ingreso y salida de equipos de la organización.*
d. *El debido control de los servicios de mantenimiento.*
e. *Los controles para el desecho y reutilización de recursos de TI.*

f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
g. El acceso de terceros.
h. Los riesgos asociados con el ambiente"

Al respecto, se le consultó a la Msi. Castro Molina, la cual indicó lo siguiente:

> "*En lo que respecta al estudio de penetración externa, la contratación está dada en términos de pruebas bajo la modalidad de caja negra, en donde no se le da ninguna pista al proveedor de las pruebas a realizar ni de la infraestructura, ya que este test consiste en realizar "ataques" por todos los medios posibles para identificar vulnerabilidades*."

La situación descrita podría ocasionar que no se evaluaran aspectos relevantes en materia de seguridad en tecnologías de información y comunicaciones como lo son sistemas de información, bases de datos, enlaces de comunicación que podrían afectar la continuidad de los servicios. Asimismo, se pueden materializar accesos y usos indebidos de la información almacenada y custodiada por la CCSS.

En ese mismo sentido, el no haber incluido áreas como las señaladas, podría haber generado un desaprovechamiento de la inversión y de la oportunidad de la contratación gestionada por la Administración, para analizar temas estratégicos en materia de seguridad informática, que pudieron aportar debilidades en los enlaces de comunicación, sistemas de información y bases de datos, entre otros.

8. SOBRE EL MONITOREO A LA EJECUCIÓN DEL ANÁLISIS DE VULNERABILIDADES

No se identificó en la documentación del expediente de contratación y en las minutas de las sesiones de trabajo de ejecución elaboradas, que se efectuara un monitoreo al avance y cumplimiento de objetivos planteados en la gestión del análisis de vulnerabilidades y riesgos de seguridad en TIC, por parte de los niveles superiores jerárquicos a la Subárea de Seguridad en Informática.

Para el caso del Área de Seguridad y Calidad de la Información, únicamente se evidenció la realización de tareas de índole administrativa, tales como trámite de pago de factura así como reuniones para valorar en su momento, una posible rescisión del contrato con el proveedor. El artículo 12, incisos a) y b) de la Ley General de Control Interno, indica sobre los deberes del jerarca y de los titulares subordinados en el sistema de control interno, 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.

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, señala con respecto a las funciones sustantivas relacionadas con la gestión estratégica del proceso de Dirección las siguientes:

"*Planificar, coordinar, controlar y evaluar a nivel macro la gestión de las áreas de trabajo adscritas y los resultados globales, con base en los procesos de trabajo aprobados, la programación operativa, los planes, los instrumentos de control establecidos y los informes de labores, con el propósito de satisfacer con oportunidad y calidad las demandas de los usuarios y definir las medidas correctivas en caso necesario."*

Asimismo, el Manual de Organización referido, indica sobre el control de objetivos y metas:

"*Realizar en conjunto con los jefes de área, sesiones de trabajo periódicas para el control de los objetivos y las metas globales de la organización, suministrar información relevante y ejercer un liderazgo participativo, con base en las políticas institucionales vigentes y los requerimientos internos, con el objetivo de retroalimentar el desarrollo de la gestión*."

Sobre las funciones sustantivas del Área de Seguridad y Calidad Informática, el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, indica:

"Determinar periódicamente el cumplimiento de los objetivos y las metas planificadas, mediante la revisión del Plan Operativo y las prioridades establecidas, con el propósito de informar al nivel superior el grado de cumplimiento de las responsabilidades asignadas."

Por otra parte, en el Manual de Organización indicado, sobre las funciones de la Subárea de Gestión de Compras de la DTIC, indica lo siguiente:

"*Vigilar que las contrataciones generadas a lo interno, se realicen en las mejores condiciones económicas y de calidad para la Institución, que satisfagan eficazmente las necesidades planificadas y que se realice el control y seguimiento necesario durante la Ejecución del contrato hasta la recepción final, mediante el cumplimiento de la regulación y la normativa técnica vigente, con el objetivo de que el gasto e inversión que se realiza sea racional y oportuno."*

Sobre la fiscalización y supervisión realizada a la ejecución de las evaluaciones y el desempeño de la firma Deloitte & Touche por parte de los niveles superiores, la Msi. Ana María Castro Molina, Encargada General del Contrato indicó:

> *"…No hubo fiscalización oficial, las consultas eran verbales y ocasionalmente se revisaron algunas minutas…"*

Asimismo, la Msi. Castro Molina mencionó actividades en las que participaron niveles superiores jerárquicos, indicando:

> *"Se dieron consultas verbales sobre el tema, asimismo, informaba verbalmente a la jefatura del Área sobre el avance del proyecto, para que ésta gestionara el trámite de las facturas.*
>
> *Asimismo, la fiscalizadora participó en la consulta verbal que se realizó a la Dirección Jurídica con respecto a la posibilidad de rescindir el contrato, así como con el apoderado generalísimo de la empresa adjudicada.*
>
> *Por iniciativa del ASCI se realizó una reunión con personal de la Dirección de TIC a saber: el Subgerente, la asesora legal y la jefatura de la Sub Área de Gestión de Compras, para valorar la rescisión del contrato·".*

La falta monitoreo de niveles superiores a la Subárea de Seguridad Informática a cargo del contrato, podría afectar el apoyo y la participación que otras unidades dentro y fuera de la Dirección de Tecnologías de Información y Comunicaciones, otorguen a la evaluación revisión de la seguridad en TIC institucional.

Por otra parte, la falta de involucramiento de las jefaturas pudo provocar que no se condujera el análisis de las vulnerabilidades con una visión integral del tema, afectando la toma de decisiones relacionadas con la ejecución del contrato, en las que su adopción y abordaje hubieran favorecido el desarrollo de las actividades, en cuanto a oportunidad y participación de los diversos actores.

La Institución realizó una importante inversión de recursos tanto económicos como humanos y materiales para realizar la contratación, por lo que no otorgarle la atención que merecen los resultados encontrados en cada una de las evaluaciones, podría significar un desaprovechamiento de los recursos limitados que dispone la CCSS, así como la posibilidad de que no se alcancen los objetivos planteados en la contratación.

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

9. RESPECTO DE LA TRANSFERENCIA DE CONOCIMIENTO

De conformidad con la documentación del expediente de contratación conformado para este proceso, no se realizó la transferencia de conocimiento conforme los términos solicitados en el pliego cartelario en cuanto a la cantidad de temas evaluados y el número de participantes de la Institución en cada una.

Esta Auditoría tuvo evidencia de únicamente dos sesiones de transferencia que brindó la empresa consultora, con participación de tres funcionarios de la Subárea de Seguridad en TI. De acuerdo con información suministrada por la Encargada General del Contrato, los temas incluidos fueron:

1. "Herramientas más utilizadas al evaluar la seguridad de dispositivos tecnológicos": la cual corresponde a la evaluación del Sistema de Gestión de la Seguridad Informática. (SGSI)

2. "Guía de evaluación de mapeo de riesgos"

Como se desprende de lo anterior, no se abordó la totalidad de los temas de las diez evaluaciones realizadas. Sin embargo, según indicó la Msi. Ana María Castro Molina, en oficio DTIC-5058-2017 del 24 de agosto del 2017, con la entrega de resultados se realizó la transferencia de conocimiento, pese a que esta Auditoría no obtuvo evidencia de lo señalado.

En el Capítulo 1 Condiciones Técnico Específicas, punto 2.6, el cartel indica:

> *"Por cada etapa finalizada, la empresa deberá brindar la transferencia de conocimiento para 8 funcionarios de la CCSS, sobre las herramientas y estándares utilizados en el trabajo realizado dentro de cada etapa para lo cual debe indicar la cantidad de horas de transferencia por etapas. El lugar de la transferencia será definido por los funcionarios de la CCSS."*

Sobre este tema, la Msi. Castro Molina señaló lo siguiente:

> "*Solo una de las fases de la contratación exigía una sesión de transferencia de conocimiento para conocer las herramientas utilizadas para las pruebas de penetración externa. Dentro de los temas abordados, se encuentran las herramientas para hacer ataques éticos, escaneo de puertos, elevación de privilegios, suplantación de usuarios, entre otras."*

La limitada participación en el proceso de transferencia de conocimiento brindado por la firma consultora contratada, no garantiza la difusión de conocimientos sobre un tema clave en la institución, como lo son herramientas y estándares utilizados por empresas con mejores prácticas en el campo de la seguridad informática. Lo anterior, no propicia generación de conocimiento en funcionarios operativos y

tomadores de decisiones, aspecto relevante para establecer un marco de seguridad informática en la CCSS.

10. DEL PLAZO DE ENTREGA DEL INFORME DEL PRIMER SEGUIMIENTO

Esta Auditoría evidenció que tanto a nivel del pliego cartelario, como en la documentación oficial de la contratación evaluada, no se definió plazo de entrega del informe referente al primer seguimiento efectuado por la firma Deloitte & Touche.

El artículo 51 del Reglamento a la Ley de Contratación Administrativa, establece respecto del cartel de la contratación lo siguiente:

> *"(…) Deberá constituir un cuerpo de especificaciones técnicas, claras, suficientes, concretas, objetivas y amplias en cuanto a la oportunidad de participar…"*

Por otra parte, ese cuerpo normativo indica en el artículo 47 relacionado con las multas y la cláusula penal lo siguiente:

> *" La Administración podrá establecer en el cartel, el pago de multas por defectos en la ejecución del contrato, considerando para ello, aspectos tales como, monto, plazo, riesgo, repercusiones de un eventual incumplimiento par el servicio que se brinde o para el interés público…"*

Las Normas Técnicas de Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, en el punto 2.1 Planificación de las Tecnologías de Información señala:

> "*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*."

En ese sentido, únicamente se identificó el oficio DTIC-1322-2017 del 8 de marzo del 2017, dirigido al Sr. Andrés Casas Cruz, Socio de la firma Deloitte & Touche, en el cual la Msi. Ana María Castro Molina, Encargada General del Contrato, indica:

> *"…en conocimiento de las múltiples situaciones que se han presentado por parte de la CCSS afectando el proceso de seguimiento, se avala la ampliación del plazo para la entrega de los productos de la fase de seguimiento 2.3.1 a) b) c) al 17 de marzo 2017, con base en lo solicitado…"*

Asimismo, se evidenciaron al menos dos prórrogas adicionales concedidas para la entrega de los productos de seguimiento, mediante oficios DTIC-3376-2017 del 8 de junio del 2017 y DTIC-4976-2017 del 22 de agosto del 2017, a través de los cuales la Encargada General del Contrato otorga como fecha final el 16 de junio del 2017 y 25 de agosto del 2017, respectivamente.

Sobre este tema, la Msi. Ana María Castro Molina, Encargada General del Contrato, indicó respecto a la gestión de seguimiento lo siguiente:

> *"El atraso en el primer seguimiento se dio entre otras cosas por disposición de recurso humano de las unidades de la Caja que debía atender los planes remediales, priorización de tareas del ASCI, cancelación de reuniones, no se aportó información, no se formalizaron las minutas por parte de los responsables de seguimiento de las actas, cambios de responsables de atender los planes remediales sin entregar documentos a quienes los sustituían, entre otras."*

Sobre la fecha de entrega del informe del primer seguimiento por parte de la firma Deloitte & Touche, la Encargada General del Contrato indicó lo siguiente:

> *"El cartel omitió la fecha de entrega para el cierre del primer seguimiento, pero en las reuniones de control semanales se definió la fecha de entrega final del estudio, según se indica en oficios DTIC-3376-2017 y DTIC-4976-2017."*

No disponer del informe del primer seguimiento en un plazo definido por el pliego cartelario, podría ocasionar desconocimiento del estado de los planes remediales solicitados para las vulnerabilidades identificadas, en detrimento de la toma de decisiones por parte de la Administración para acelerar los procesos de atención.

Lo anterior, podría generar que se materialicen riesgos por falta de atención oportuna a las acciones de mitigación. Asimismo, la administración no puede efectuar los pagos a la firma contratada por concepto de primer seguimiento, conforme lo programado, en virtud de que no dispone del entregable pactado.

11. SOBRE EL CUMPLIMIENTO DE LOS PLANES REMEDIALES

De acuerdo con el documento del primer seguimiento entregado por la empresa consultora el 16 de junio del 2017 y remitido a esta Auditoría el 20 de junio del 2017, el cumplimiento de los planes remediales establecidos como mecanismos para mitigar las vulnerabilidades identificadas fue de un 15%, es decir, de 1301 acciones planteadas por la Firma Deloitte & Touche para corregir las riesgos en las diferentes tipos de evaluaciones realizadas, se encuentran pendientes de atender 899 y deben valorarse

207 acciones para determinar el criterio de no aplicabilidad otorgado en este seguimiento por funcionarios de la CCSS. Lo anterior se especifica en la tabla incluida a continuación:

Tabla 5
Estado de los planes remediales

Acciones remediales	Corregidas	Pendientes	No aplican	Total
Cantidad	195	899	207	1301
Porcentaje	15%	69%	16%	100%

Fuente: *Primer seguimiento efectuado por Deloitte &Touche*

A manera de resumen, se presenta en el siguiente cuadro, el nivel de cumplimiento de las acciones de los planes remediales de las vulnerabilidades identificadas, correspondientes a cada una de las etapas de la contratación:

Tabla 6
Cumplimiento de acciones por fases evaluadas

Etapas	No Aplica	Corregidas	Pendientes
Evaluación Sistema de Gestión de Seguridad Informática	20%	31%	49%
Pruebas de Penetración Externa	0%	33%	67%
Evaluación Ingeniería Social	33%	67%	0%
Evaluación Penetración Interna	0%	26%	74%
Evaluación de Infraestructura Tecnológica	0%	36%	64%
Evaluación de equipos médicos	0%	5%	95%
Evaluación de Call Center	62%	15%	23%
Evaluación Red de Telefonía	5%	41%	54%
Evaluación Sistemas de Información	39%	12%	49%
Evaluación Física	0%	38%	62%

Fuente: *Informe de primer seguimiento Deloitte & Touche*

Llama la atención que en dos de las evaluaciones efectuadas no se generó ningún avance o cumplimiento, tal es el caso de las mencionadas seguidamente:

- Equipos médicos Hospital San Juan de Dios
- Equipos médicos Hospital San Vicente de Paúl

Además, para el Test de Penetración Interna realizado en la Gerencia de Pensiones el cumplimiento de las acciones fue de un 5% y en oficinas centrales para este tipo de revisión, se alcanzó el 10% de planes remediales efectuados.
En el Anexo 1, se muestra el detalle del avance en la atención de las acciones propuestas para mitigar las vulnerabilidades de las etapas realizadas en los centros de salud y en la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

La Ley General de Control Interno, en su artículo 12, Deberes del Jerarca y de los titulares subordinados en el sistema de control interno, en los puntos a) y b) señala:

> *"En materia de control interno, al jerarca y a 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 acciones correctivas, ante cualquier evidencia de desviaciones o irregularidades…"*

Las Normas Técnicas para la Gestión y Control de Tecnologías de Información, señalan en el punto 1.3 Gestión de Riesgos, lo siguiente:

> *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."*

Las Directrices para la Contratación de Servicios de Auditoría Externa en el Sector Público" (D-3-2009-CO-DFOE), emitidas por la contraloría General de la República, señalan en el punto 8. Atención de observaciones y recomendaciones, lo siguiente:

> "*La Administración debe instaurar los procedimientos pertinentes para el análisis de los resultados de los servicios de auditoría externa, y para la implantación de las observaciones y recomendaciones correspondientes, dentro del plazo previsto por el ordenamiento jurídico, así como para el respectivo seguimiento. Como parte de lo anterior, debe definir los responsables y los plazos razonables para cumplir con tales tareas."*

Al respecto, en el documento denominado "Estrategia para la mejora de la implementación de los hallazgos", preparado por Deloitte & Touche y entregado por la Msi. Ana María Castro Molina, Encargada General del Contrato, a este Ente de Fiscalización, se indica lo siguiente:

> *"Durante el proceso de entrevistas y revisión de la adopción de recomendaciones concernientes a la mejora de las capacidades de seguridad de la información de las TIC en la CCSS, se*

identificaron situaciones que limitaron la implementación de las recomendaciones. A continuación, se detallan dichas situaciones:

- *Funcionarios a los cuales se les entregaron los informes originalmente, durante los años 2015-2106, se trasladaron a otras áreas de la institución y los informes no fueron remitidos a los funcionarios que asumieron los cargos. Debido a esta situación se dieron entrevistas en las cuales se desconocían los hallazgos y por ende las recomendaciones. Identificando avance nulo en estos casos.*
- *Los responsables no transmiten de forma granular la información, por lo cual los involucrados en la implementación de los hallazgos de forma técnica, desconocen los mismos y las observaciones asociadas.*
- *Falta de sensibilidad ante el impacto de los hallazgos, durante las entrevistas se identificaron encargados, que brindaban el mismo nivel de prioridad a las recomendaciones, aun cuando los informes indicaban el nivel de riesgos de los mismos.*
- *Durante la evaluación se identificaron múltiples equipos presentaban una pronunciada obsolescencia tecnológica, lo cual no permitía a los administradores la implementación de las recomendaciones técnicas".*

Al respecto se le consultó a la Msi. Castro Molina, señalando lo siguiente:

"El porcentaje de cumplimento fue bajo, entre otras cosas por disposición de recurso humano de las unidades de la Caja que debía atender los planes remediales, priorización de tareas del ASCI, cancelación de reuniones, no se aportó información, no se formalizaron las minutas por parte de los responsables de seguimiento de las actas, cambios de responsables de atender los planes remediales sin entregar documentos a quienes los sustituían, entre otros."

El no brindar una atención oportuna a los planes remediales propuestos para mitigar las vulnerabilidades identificadas podría ocasionar que se materialicen los riesgos identificados con la consecuente afectación a la prestación de servicios que se brinda a los asegurados tanto de salud como de pensiones.

Asimismo, no tomar las medidas correspondientes para subsanar las oportunidades de mejora evidenciadas en el informe entregado por la firma Deloitte & Touche, podría ocasionar que el porcentaje de cumplimiento se mantenga bajo durante el próximo seguimiento a las evaluaciones indicadas en párrafos anteriores, en detrimento de la continuidad de los servicios institucionales brindados a los asegurados y patronos por medio de las TIC.

En ese mismo orden de ideas, considerando que el pliego cartelario estableció únicamente dos seguimientos por parte de la firma consultora, la atención inoportuna de los planes remediales podría ocasionar que la Institución deba destinar recursos asignados a otras labores sustantivas para la finalizar

la implementación de las acciones recomendadas por el contratista, así como para brindar la gestión de asegurar su cumplimiento.

12. SOBRE EL ACOMPAÑAMIENTO SOLICITADO POR UNIDADES INSTITUCIONALES

Esta Auditoría identificó oportunidades de mejora en el acompañamiento y colaboración solicitados por unidades a las cuales se remitieron planes remediales por atender, producto de la evaluación de vulnerabilidades. Lo anterior se evidencia en los casos que se mencionan a continuación:

- En el caso de las acciones de mejora propuestas para el Portal de Recursos Humanos, mediante oficio SSARH-0021-2016 del 4 de mayo del 2016, la Master Laura Paz Morales, Jefe Subárea Sistema Automatizado en Recursos Humanos, le indicó a la Encargada General del Contrato lo siguiente:

  "(…) se identifican cuatro vulnerabilidades en el Portal de Recursos Humanos que se relaciona con temas de seguridad en el desarrollo de sistemas automatizados…"

  "(…) la suscrita desconoce de la existencia de dichas políticas o de la metodología de desarrollo seguro y tampoco se ha logrado recabar información en la intranet por lo que se solicita, instruya a esta unidad sobre esos temas o se facilite documentación necesaria para su aplicación en el Portal de Recursos Humanos."

Sin embargo, al momento de la revisión realizada por esta Auditoría el 31 de marzo del 2017, no se evidenciaron acciones concretas por parte de la Msi. Ana María Castro Molina, Encargada General del Contrato, tendientes a apoyar a esa unidad, observándose al respecto, únicamente el traslado de la nota por parte de esa funcionaria al contratista Deloitte & Touche.

- Mediante oficio DCO-0385-2016 del 26 de abril del 2016, el Lic. Luis Diego Calderón Villalobos, Director de Cobros, le indica al Lic. Robert Fabricio Picado Mora, Subgerente de Tecnologías de Información y Comunicaciones lo siguiente:

  "*Para la atención de los siguientes hallazgos se requiere la colaboración de las diferentes áreas o subáreas de la DTIC, ya que a nivel de CGI local para la mayoría de los casos no se cuenta con los suficientes privilegios de usuario para realizar los cambios solicitados."*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, indica en cuanto a gestión estratégica de la Dirección de Tecnologías de Información y Comunicaciones, lo siguiente:

"*Otorgar asesoría técnica, con base en la demanda de los diversos niveles de la organización, con la finalidad de lograr un desarrollo armónico y efectivo de la gestión institucional en el área de competencia.*"

En ese mismo Manual, se indica la obligatoriedad del Area de Seguridad y Calidad Informática de asesorar a los Centros de Gestión Informática, de la siguiente manera:

"Asesorar y evaluar a los centros de gestión informática de nivel regional, gerencial y local de acuerdo con la normativa técnica, los protocolos, los estándares, las políticas y las estrategias vigentes en su ámbito de competencia, con la finalidad de lograr el desarrollo efectivo y verificar el cumplimiento efectivo de los lineamientos establecidos."

Al respecto, la Msi Castro Molina indicó:

"…La nota de RRHH se canalizó directamente con el contratista como parte del seguimiento, esta gestión se ve reflejada en el primer seguimiento; el caso del oficio de la Dirección de Cobros, éste se envió directamente a la DTIC, la cual le consultó directamente a la Sub Área de Seguridad en TI, la cual asesoró que el CGI de la Dirección de Cobros escalara su solicitud al CGI de la Gerencia Financiera para la atención de los hallazgos."

La situación descrita podría ocasionar que las unidades no corrijan o aceleren el proceso de implementación de planes remediales, por falta de asesoría y apoyo, en detrimento de la seguridad en TIC, por una posible materialización de riesgos que afectan la prestación de los servicios. Asimismo, la falta de apoyo no propicia un ambiente de control para los funcionarios a cargo de atender las acciones propuestas, lo cual no contribuye a que la Caja disponga de una cultura de seguridad informática.

13. SOBRE LA CONFORMACIÓN DEL EXPEDIENTE DE CONTRATACIÓN

En la revisión efectuada al expediente de ejecución de la contratación directa 2014CD-000003-1150, "Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC", esta Auditoría constató que el legajo conformado, presentaba al menos las siguientes debilidades:

- El expediente no estaba actualizado, no contenía la documentación relacionada con la fase de seguimiento, entre otros documentos faltantes.
- El expediente se encontraba incompleto, pues no constaban notas de respuesta a solicitudes del contratista, minutas de reuniones, oficios entre unidades de la Caja.
- Documentos sin foliar.
- Borradores en el expediente o documentos corregidos con lapicero.
- Documentos y oficios duplicados.

- El orden de foliación del expediente no correspondía al orden en que ocurrieron los hechos, es decir no refleja la cronología de los eventos del proceso de contratación y su ejecución.
- Documentos de pagos y otros de carácter administrativo archivados en expediente diferentes.
- Documentos sin firmas.

Al respecto, el Reglamento de la Ley de Contratación Administrativa indica en su artículo 11, sobre el expediente, lo siguiente:

> *"Una vez tramitada la decisión inicial, se conformará un expediente por la Proveeduría como unidad encargada de su custodia. Dicho expediente deberá estar debidamente foliado y contendrá los documentos en el mismo orden en que se presentan por los oferentes o interesados, o según se produzcan por las unidades administrativas internas. Los borradores no podrán formar parte de dicho expediente.*
>
> *La incorporación de los documentos al expediente no podrá exceder de dos días hábiles una vez recibidos por la Proveeduría. Para ello, la Administración, deberá adoptar las medidas necesarias a fin de cumplir la actualización del expediente. Las dependencias internas deberán remitir los estudios dentro de los dos días hábiles siguientes a su emisión."*

El Manual de Organización de la DTIC, en las funciones de la Subárea de Gestión de Compras, señala lo siguiente:

> "*Vigilar que las contrataciones generadas a lo interno, se realicen en las mejores condiciones económicas y de calidad para la Institución, que satisfagan eficazmente las necesidades planificadas y que se realice el control y seguimiento necesario durante la Ejecución del contrato hasta la recepción final, mediante el cumplimiento de la regulación y la normativa técnica vigente, con el objetivo de que el gasto e inversión que se realiza sea racional y oportuno."*

Sobre este tema, se le consultó a la Encargada General del Contrato, la cual señaló lo siguiente:

> *"(…) es importante señalar que las cargas de trabajo y limitación de recurso humano dificultan la atención de situaciones como esta, en ese sentido, sería recomendable realizar una sesión para actualizar conocimientos en materia de contratación administrativa"*

No disponer de un expediente actualizado, ordenado y completo dificulta la gestión de la adquisición de bienes y servicios, así como la ejecución contractual, entre otras razones, por la dificultad de ubicar documentos y ejecutar los procesos de adquisición de bienes y servicios conforme lo indicado en el cartel, ocasionando incumplimiento a la normativa en esta materia. Adicionalmente, no se dispone de la

información completa para adoptar oportunamente decisiones que el procedimiento requiere para continuar sin dilaciones.

La conformación de un expediente debidamente foliado, de acuerdo con lo establecido en la normativa, minimiza la posibilidad de cometer errores de trámite, garantizando transparencia y seguridad jurídica a los participantes del proceso.

CONCLUSIONES

La información, en conjunto con los procesos, sistemas y aplicaciones que la utilizan son activos de gran importancia para la institución, por lo que mantener la confiabilidad, integridad, así como la disponibilidad de los datos es relevante para garantizar la eficiencia, calidad y oportunidad de los servicios de salud, pensiones y prestaciones sociales.

La existencia de un número importante de amenazas en la infraestructura de red y recursos informáticos de una organización obligan a que los mismos, deban estar protegidos y mitigados bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo, por lo que garantizar que los recursos tecnológicos estén disponibles y confiables para cumplir sus objetivos, debe ser uno de los retos y prioridades de la CCSS.

En virtud de lo anterior, y considerando la trascendencia del análisis de vulnerabilidades y riesgos de la seguridad en TIC contratado, este Órgano de Fiscalización identificó oportunidades de mejora en su gestión.

En primera instancia, la contratación administrativa constituye un medio para alcanzar las metas y objetivos planteados por la institución, por ello la planificación es clave para dar la debida atención a la necesidad que se va a satisfacer, en ese sentido, la Dirección de Tecnologías de Información y Comunicaciones debió asegurar el requerimiento que tenía la Caja de evaluar las vulnerabilidades de la red de telefonía y el Call center de la Gerencia de Pensiones de forma tal que estuvieran disponibles durante la ejecución, como parte del objeto de revisión del estudio contratado.

Por otra parte, preocupa a esta Auditoria que acciones propuestas con base a las vulnerabilidades no fueran dirigidas a las unidades competentes, pudieran ser inaplicables o en su defecto, no existieran los riesgos a que se hace referencia. De haber involucrado en el proceso de revisiones previas de los productos generados, a especialistas y funcionarios con la competencia, para cada uno de los temas abordados, situaciones como las mencionadas se hubiesen disminuido para así disponer de un informe oportuno que reflejara la realidad de las vulnerabilidades de la Institución.

En ese mismo sentido, debido a la cantidad de vulnerabilidades que evidenciaron los diferentes productos entregados por la empresa, el número de unidades evaluadas y las múltiples acciones recomendadas en los planes remediales a ejecutarse, es necesario el involucramiento, apoyo y compromiso de niveles superiores, Direcciones de hospitales, Gerencias y de la Dirección de Tecnologías de Información y Comunicaciones.

Sobre el apoyo estratégico en prácticas de seguridad de la información en la CCSS, en el informe ATIC-049-2014, esta Auditoría había señalado, que las políticas, directrices y procedimientos establecidos en esa índole son de aplicabilidad institucional y por lo tanto debe tener el apoyo e impulso de los altos niveles organizacionales, aspecto que no se apreció en este estudio.

Por otra parte, la transferencia de conocimiento no se realizó conforme la normativa aplicable, gestión que se considera vital en las organizaciones, las cuales deben ser capaces de adquirir, generar y utilizar el conocimiento y, por lo tanto, en el caso auditado, es fundamental transferirlo formalmente a los involucrados en el proceso, en beneficio de la propia institución.

Con relación a la ejecución de los planes remediales el primer seguimiento se determinó un cumplimiento de un 15% para atender los riesgos identificados, por lo que es preciso que la Institución diseñe una estrategia que le permita acreditar las acciones que mitigan los riesgos y vulnerabilidades se realicen con celeridad y contundencia.

A criterio de este Órgano de fiscalización, se determinaron debilidades de conducción en la gestión del análisis de vulnerabilidades, así como la falta de un proceso de revisión de los hallazgos en cada etapa, previa a su comunicación.

En ese orden de ideas, es preciso considerar que se determinaron vulnerabilidades como obsolescencia de versiones, controles en los sistemas, políticas, metodologías, documentación técnica, prácticas o configuraciones, las cuales pueden ser tratadas, a criterio de la firma Deloitte & Touche, con recursos que no representarían un mayor esfuerzo, sin embargo, con respecto a este tipo de actividades tampoco se acreditó el cumplimiento.

Por otra parte, debido al alcance cubierto por la evaluación realizada, no se analizaron las condiciones de seguridad tecnológica en todos los hospitales, direcciones y demás unidades de la CCSS, es importante que la Gerencia de Infraestructura y Tecnologías, y la Dirección de Tecnologías de Información y Comunicaciones valoren la conveniencia de brindar un abordaje integral a las vulnerabilidades encontradas, incluyendo, entre otras acciones, la emisión de políticas que minimicen los riesgos identificados, así como la definición de herramientas y metodologías para analizar en conjunto con funcionarios expertos e instancias que se estime pertinente, los planes de mejora propuestos y los hallazgos incluidos en los productos obtenidos en la evaluación contratada. Lo anterior con el propósito

de fortalecer la seguridad en tecnologías de información de la CCSS, en aprovechamiento de la inversión efectuada y de los servicios profesionales expertos adquiridos.

En lo que respecta a los planes remediales pendientes de atender, se identificaron vulnerabilidades recurrentes que podrían generar un impacto considerable en la operación de la institución en caso de ser explotadas, por lo que la planificación debe establecer prioridades para la implementación.
Cada vez se comparten y utilizan más datos para la prestación de los servicios institucionales en todo el territorio nacional, muchos de ellos son transportados en diversas redes y utilizados tanto por usuarios externos como internos, por lo que un uso inadecuado de la información que se trasiega en sistemas, plataformas tecnológicas y en la nube puede significar desde pérdida de información, interrupción del servicio hasta erogaciones millonarias por transacciones no autorizadas y sufrir perjuicios no solo de imagen sino también comprometiendo la calidad de la prestación de servicios otorgados a la población costarricense, razón por la cual la seguridad en las TIC es relevante en la CCSS.

En razón de lo anterior, esta Auditoría propone una serie recomendaciones con el fin de apoyar a la Administración Activa en el proceso de gestión de vulnerabilidades y riesgos de seguridad en tecnologías de información y comunicaciones.

RECOMENDACIONES

A LA ARQ. GABRIELA MURILLO JENKINS, EN SU CALIDAD DE GERENTE DE INFRAESTRUCTURA Y TECNOLOGÍAS O A QUIEN OCUPE SU CARGO

1. De acuerdo con lo evidenciado en el presente estudio, esa Gerencia en coordinación con la Dirección de Tecnologías de Información y Comunicaciones, deberá valorar la integración de un equipo interdisciplinario encargado de analizar los hallazgos planteados en el presente informe estableciendo las acciones que se estime pertinentes conforme derecho corresponda de acuerdo con las causas brindadas por los funcionarios a cargo de la gestión de la evaluación de vulnerabilidades contratada.

   Así mismo, dicho equipo deberá conformar un plan de acción orientado a la subsanación de los aspectos señalados según se considere viable desde el punto de vista normativo aplicable, considerando al menos los siguientes temas para las etapas vigentes del contrato:

   - Involucramiento de personal especializado.
   - Monitoreo a la ejecución contractual.
   - Transferencia de conocimiento formalizado a la Administración de acuerdo con los términos establecidos en el cartel de contratación.
   - Seguimiento al cumplimiento de los planes remediales.

- Acompañamiento a las unidades institucionales.
- Conformación del expediente de contratación.
- Otros elementos que la Administración Activa considere conveniente incluir.

Esa Gerencia deberá analizar el plan y formalizarlo, con el fin de establecer los mecanismos de control que se estimen necesarios para impulsar el cumplimiento de las acciones incluidas en ese documento.

Para acreditar el cumplimiento de esta oportunidad de mejora, deberá remitirse a este Órgano de Fiscalización, en un plazo de tres meses, a partir del recibo del presente informe, el plan de acción aprobado por esa Gerencia, así como la documentación de los mecanismos definidos oficialmente para garantizar su cumplimiento.

2. Instruir al equipo de trabajo conformado en atención de la recomendación uno del presente informe, elaborar 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. Lo anterior en aras del fortalecimiento de la seguridad informática de la CCSS.

   El análisis mencionado deberá incluir al menos los siguientes elementos:

   - Impacto y probabilidad de ocurrencia de las vulnerabilidades.
   - Recurso Humano requerido para la atención de las acciones.
   - Recursos financieros necesarios.
   - Tiempo requerido para la ejecución de las acciones remediales
   - Otros aspectos que la Administración Activa considere conveniente incluir.

   La estrategia definida deberá ser remitida a esa Gerencia para realizar la valoración integral de los riesgos de acuerdo con una priorización fundamentada en términos de impacto institucional.

   Así mismo, se deberán establecer los mecanismos de control que correspondan para monitorear y dar seguimiento a la materialización de medidas propuestas en la estrategia mencionada.

   Para acreditar el cumplimiento de esta recomendación, deberá remitirse a esta Auditoría, en un plazo de cuatro meses, a partir del recibo del presente informe, la estrategia aprobada por esa Gerencia, así como la documentación de las acciones ejecutadas con fundamento en la revisión y análisis solicitados, así como el monitoreo al cumplimiento de esa estrategia.

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

Al MÁSTER ROBERT PICADO MORA, EN SU CALIDAD DE SUBGERENTE DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O A QUIEN OCUPE SU CARGO

3. De acuerdo a los resultados del presente informe y debido a la necesidad de mejora continua en la gestión de cultura de TI institucional, en conjunto con el Área de Seguridad y Calidad Informática deberá establecer un plan orientado a socializar en lo que se estime conveniente, los resultados de las revisiones efectuadas por la firma consultora, así como mejores prácticas utilizadas, con el fin de promover concienciación sobre la importancia de la seguridad en las TIC en la CCSS.
   Lo anterior mediante el uso de metodologías y/o herramientas disponibles tales como talleres, videoconferencias, capacitaciones, boletines u otros.

   Así mismo, se deberán establecer los mecanismos de control que correspondan para monitorear y dar seguimiento a la materialización de las actividades propuestas en el plan mencionado.

   Para acreditar el cumplimiento de esta oportunidad de mejora, deberá remitirse a esta Auditoría en un plazo de tres meses a partir del recibo del presente informe, el plan de socialización formalizado, así como los mecanismos de control establecidos para garantizar su atención.

4. Generar una directriz y/o lineamiento orientado a regular actividades mínimas de apoyo a la planificación y ejecución contractual que deben considerarse en futuras contrataciones relacionadas con evaluación de vulnerabilidades de seguridad en TIC, de acuerdo con los aspectos abordados en el Apartado de Hallazgos, así como de los resultados obtenidos en el plan desarrollado en cumplimiento de la recomendación uno del presente informe, con el fin de garantizar la atención de los objetivos planteados, así como un aprovechamiento razonable de la inversión efectuada, a fin de que este tipo de contrataciones contribuyan al fortalecimiento de la seguridad informática institucional.

   Para acreditar el cumplimiento de esta oportunidad de mejora, deberá remitirse a esta Auditoría en un plazo de tres meses a partir del recibo del presente informe, la directriz o lineamiento oficializado por esa Dirección, así como su correspondiente divulgación e instrucción para su aplicación.

5. Instruir a la Subárea Gestión de Compras para que en conjunto con los funcionarios que estime conveniente, analice las debilidades detectadas en la ejecución de la contratación evaluada, a fin de generar políticas y directrices, así como procesos de capacitación y asesoría a los funcionarios de la DTIC según corresponda, con el fin de orientar las funciones y actividades que deben considerarse en el cumplimiento del rol de Administrador y/o Encargado de Contrato.

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

Para acreditar el cumplimiento de esta oportunidad de mejora, deberá remitirse a este Órgano de Fiscalización, en un plazo de tres meses a partir del recibo del presente informe, las políticas y/o directrices oficializadas, así como el plan de asesoría y capacitación correspondiente.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, se procedió a comentar los resultados del presente informe el 22 de setiembre del 2017, con el Máster Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones y el Ing. Jorge Porras Pacheco, Asesor de la Gerencia de Infraestructura y Tecnologías, quienes no señalaron observaciones respecto de lo indicado en los hallazgos del estudio.
En lo que respecta a las recomendaciones, la Administración solicita se incluya dentro de los elementos a valorar en el análisis solicitado en la recomendación dos, el tema de recursos financieros requeridos para atender los planes remediales propuestos por la firma consultora. En ese sentido, considerando que es razonable lo indicado, es criterio de este Órgano de Fiscalización realizar el ajuste solicitado. Respecto de las recomendaciones uno, tres, cuatro y cinco, no se emitieron observaciones.

ÁREA TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIONES

IDANNIA MATA SERRANO (FIRMA)
Firmado digitalmente por IDANNIA MATA SERRANO (FIRMA)
Fecha: 2017.10.06 11:36:55 -06'00'

Licda. Idannia Mata Serrano
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2017.10.06 15:53:18 -06'00'

Lic. Rafael A. Herrera Mora
JEFE DE ÁREA

OSC/RHM/IMS/lbc

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

Anexo 1
Cumplimiento de acciones por Unidad de aplicación

Etapas	Total de acciones remediales	No Aplica	Pendiente	Corregido	Porcentaje de incumplimiento
Evaluación al Sistema de Gestión de la Seguridad Informática	116	23	57	36	49%
Pruebas de Penetración Externa	15	0	10	5	67%
Pruebas de ingeniería social	3	1	0	2	67%
Pruebas de penetración interna Data Center	23	5	17	1	74%
Pruebas de penetración interna Gerencia de pensiones	35	0	32	3	95%
Red inalámbrica Gerencia de Pensiones	6	0	2	4	33%
Pen test Interno Hospital Dr. Rafael Angel Calderón Guardia	22	0	0	22	100%
Red Inalámbrica Hospital Dr. Rafael Angel Calderón Guardia	8	0	0	8	100%
Pen test Interno Hospital Monseñor Sanabria	31	0	24	7	77%
Pen test Interno Oficinas Centrales	67	0	60	7	90%
Evaluación Infraestructura tecnológica	62	2	38	22	61%
Evaluación de equipos Médicos Hospital Nacional de Niños	84	0	81	3	97%
Evaluación de equipos Hospital San Juan de Dios	191	0	191	0	100%
Evaluación Equipo Médico Hospital San Vicente de Paúl	90	0	90	0	100%
Servidores de Telefonía	52	32	12	8	23%

Fuente: *Informe de primer seguimiento Deloitte & Touche*