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

Al contestar refiérase a: **ID-134488**

AD-ATIC-0018-2025
17 de marzo de 2025

Máster
Robert Picado Mora, subgerente

Ingeniero
Daniel Berrocal Zuñiga, jefe
Área de Seguridad y Calidad Informática
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimados señores:

ASUNTO:	**Oficio de Advertencia referente al acceso público de información que podría catalogarse como sensible o de acceso restringido, registrada en el expediente digital de la Licitación Nacional 2022LN-000003-0001101150 "Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)"**

Esta Auditoría, en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo 2025 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, procede a pronunciarse sobre los posibles riesgos generados por el acceso público de información que podría catalogarse como sensible o de acceso restringido, según lo indicado por el proveedor en documentación consignada en la etapa de ejecución contractual de la Licitación Pública Nacional 2022LN-000003-0001101150 "Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)" y registrada en el expediente digital del Sistema Integrado de Compras Públicas (SICOP) .

Al respecto, los resultados obtenidos son los siguientes:

I. ANTECEDENTES

Mediante la Licitación Pública Nacional 2022LN-000003-0001101150 la Caja Costarricense de Seguro Social adjudicó a la empresa DELOITTE & TOUCHE SOCIEDAD ANONIMA el objeto contractual *"Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)"*, por un monto de $1.200.339,36 (Un millón, doscientos mil, trescientos treinta y nueve dólares con treinta y nueve centavos).

En relación con lo anterior, dentro de la Justificación de la procedencia de la contratación se establecen, entre otros, los siguientes aspectos:

> *"(…) Un SOC es responsable del monitoreo en tiempo real de eventos de seguridad, y de garantizar de que los posibles incidentes de ciberseguridad se identifiquen, analicen, defiendan, investiguen e informen proactivamente y no reactivamente.*

La Institución cuenta con ambientes tecnológicos críticos, los cuales son de suma importancia para la operación de la Caja Costarricense de Seguro Social, dichos ambientes se localizan en el Data Center principal (Codisa), Data Center del Instituto Costarricense de Seguridad (ICE) en Guatuso o bien, en el Centro de Computo ubicado en el piso 11 del edificio Jenaro Valverde (…)

Dichos ambientes tecnológicos a parte del gran volumen de información confidencial que manejan también están en constante interacción con el medio exterior de la institución (aplicaciones, correo, entre otros), volviéndose así ambientes sumamente vulnerables a ataques maliciosos provenientes de cualquier parte del mundo.

Dado lo anterior, se hace necesario contar con un SOC, que le permita a la institución contar con un mecanismo para la detección y respuesta a incidentes de ciberseguridad de forma proactiva, lo cual abre la posibilidad de que al sufrir un incidente, los funcionarios responsables en la institución no puedan conocerlo de inmediato y el evento escale a convertirse en una catástrofe, adicionalmente, al no contar con un insumo que permita conocer los agentes de ataque que impactan a la CCSS, las medidas de seguridad que se deseen implementar corren con la posibilidad de no ser lo suficientemente efectivas y que esto conlleva una inversión elevada en recursos que no estarán protegiendo efectivamente a los activos tecnológicos (…)".

II. RESULTADOS OBTENIDOS

Mediante oficio AI-0255-2025 del 5 de febrero de 2025 se comunicó al Máster Robert Picado Mora, subgerente de la Dirección Tecnologías de Información y Comunicaciones la ejecución del estudio "Auditoría de carácter especial sobre el desarrollo de aplicaciones y/o sistemas de información mediante software libre en la CCSS".

Como parte de los procedimientos establecidos en el estudio anteriormente citado, se realizó la revisión y análisis de algunos de los documentos que conforman expediente de contratación 2022LN-000003-0001101150 *"Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)"*, observándose en el Sistema Integrado de Compras Públicas (SICOP) la posibilidad de acceso y descarga de documentación correspondientes al "01. DTT Plan de trabajo SOC – CCSS" e "Informe mensual del servicio" elaboradas por la empresa Deloitte -proveedora de los servicios-.

En relación con lo anterior, preocupa a esta auditoría la posibilidad de acceso público y descarga en el SICOP del "Plan de trabajo SOC – CCSS" donde se consigna información referente a la entrega del servicio, la estrategia de administración del proyecto, riesgos, plan de comunicación, acuerdos de nivel de servicio, entre otros; asimismo, en el citado documento se indica la confidencialidad de los datos contenidos, de la siguiente manera:

"(…) Confidencialidad

La información de este documento es de carácter confidencial y está protegido por el contrato de confidencialidad entre Caja Costarricense de Seguro Social (En adelante "CCSS") y Deloitte, ya que cuenta con información y otros datos que no deberían ser de

conocimiento general. El documento es únicamente para uso exclusivo interno de CCSS y no debe ser utilizado con ningún otro propósito.

Por lo cual se le informa a la administración de CCSS tener presente la responsabilidad de los riesgos asociados a la fuga, exposición o mal uso de los datos descritos en este documento.

Se le entrega a CCSS con reserva de que no será usado, divulgado o reproducido salvo el propósito de su conocimiento y evaluación, para los fines previamente acordados, salvo autorización explícita y por escrito de Deloitte (…)".

Por otra parte, en dicha revisión, se evidenció la posibilidad de acceso público y descarga de los *"Informes mensuales del servicio"* de los periodos de octubre a diciembre 2023 y de enero a diciembre 2024, donde la empresa Deloitte consigna información respecto a los riesgos evidenciados, amenazas, vulnerabilidades, entre otros datos; lo anterior, producto de los análisis y evaluaciones de seguridad realizados en la institución.

Llama la atención de esta auditoría que, en el Sistema Integrado de Compras Públicas se consigna para cada uno de estos *"Informes mensuales de servicio",* un oficio del proveedor donde comunica al administrador del contrato de la CCSS que, dicho informe ha sido cargado en el **repositorio seguro** de sharepoint acordado para este fin, sin embargo, esta documentación se encuentra disponible al público en el expediente digital del SICOP, situación que genera dudas o incertidumbre sobre su posible confidencialidad o acceso restringido debido a la información y datos contenidos en ellos, que podrían catalogarse como de conocimiento y uso exclusivo interno de la institución.

En relación con lo anterior, es importante mencionar que, en el informe ATIC-0088-2023 *"Auditoría de carácter especial referente a la adquisición y dotación de soluciones tecnológicas en el ámbito de ciberseguridad"* del 20 de noviembre de 2023, este órgano de fiscalización, en el hallazgo 6 de la citada evaluación, evidenció la carencia -en el expediente electrónico de SICOP- de documentación considerada de **carácter público** referente a la ejecución contractual de la compra directa 2021CD-000007-0001101150 *"Solución Tecnológica para Seguridad Perimetral"*; recomendándose en ese momento, la implementación de mecanismos de control que garantizaran la incorporación de estos datos, conforme a lo establecido en la Ley General de Contratación Pública, su reglamento y normativa interna institucional.

Sin embargo, lo evidenciado en el informe ATIC-0088-2023, difiere a la situación detectada por esta auditoría en el expediente digital de la contratación 2022LN-000003-0001101150 "Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)", ya que, en el presente caso, además de incluirse los oficios de entrega de los informes mensuales y las actas de recepción definitiva (información considerada de carácter público), se incluyeron documentos que podrían ser de carácter confidencial y de acceso restringido, debido a los riesgos de exposición o mal uso de los datos descritos dentro de ellos, según lo indicado por la empresa Deloitte.

Actualmente existen muchos riesgos en el ámbito tecnológico, donde ciberdelincuentes sin escrúpulos intentan acceder a los datos críticos e información confidencial de las empresas, razón por la cual, día con día se requiere aumentar las medidas de seguridad para mantener dicha información bajo un adecuado resguardo y control.

III. CONSIDERACIONES NORMATIVAS.

Las Normas de Control Interno para el Sector Público, en el inciso 1.4.5 sobre el control de Accesos, refieren:

> *"La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información (…)*
> *i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios (…).*
> *Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones".*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el apartado XI. Seguridad y ciberseguridad, lo siguiente:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
>
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…)".*

En el cartel de la contratación 2022LN-000003-0001101150 "Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)", en el Capítulo I Condiciones Técnico – Especificas, apartado 14. Cláusula de Confidencialidad, numeral 14.3, se estableció, lo siguiente:

> *"Se declara confidencial de acuerdo con el artículo 139, inciso H, del Reglamento a la Ley de Contratación Administrativa, la ejecución contractual del presente proceso, por cuanto se brindará acceso a datos sensibles a los consultores aportados por el contratista".*

Además, en el apartado 15. Cláusula de discreción, confidencialidad y derechos de autor, numeral 15.1, se indicó:

> *"Conforme a lo dispuesto por la Junta Directiva de la Institución en el oficio 30829 del 14 de septiembre de 2005, los oferentes y contratistas que participen en esta compra de servicios deben*
> *comprometerse formalmente a lo que exige la institución en este campo:*

"En virtud de lo dispuesto por la Junta Directiva en el artículo 25 de la Sesión Nº 7918, celebrada el 16 de diciembre del año 2004, la o las empresas que resulten adjudicadas, que entregaran o desarrollaran productos que tengan que ver con Tecnologías de Información y Comunicación, se debe comprometer a mantener la mayor reserva, discreción y secreto, respecto a todos los datos,
diagramas, documentación, procesos y esquemas de cualquier índole (independiente del medio o formato por el que le hayan sido facilitadas) respecto de los cuales tuviere conocimientos o información en virtud de los servicios que les suministre a la Caja o bien a sus alianzas estratégicas.

La empresa contratista deberá asegurarse que su personal cumpla con esta normativa, dado que será la responsable del uso de dicha información, tanto por parte de su personal como del uso o divulgación que le den terceras personas sin el consentimiento previo por parte de la Caja. Queda prohibido a la contratista y consecuentemente a su personal, revelar a cualquier tercero sin el previo aviso y expreso consentimiento de la Caja, cualquier dato o información al que se haya tenido acceso con ocasión de la presente contratación o por el desempeño de su personal en las
labores contratadas, o bien utilizar la información para cualquier otro fin que no sea el estipulado en el contrato, todo lo anterior bajo pena de tener por incumplido el contrato sin responsabilidad alguna por parte de la Caja, pudiendo está ante un eventual incumplimiento reclamar los daños y perjuicios que el incumplimiento pudiere irrogarle, ya sea en sede administrativa o en sede judicial.

Cualquier producto que se genere durante el periodo de la contratación será propiedad de la Caja, por lo que los contratistas no pueden disponer de estos para cualquier otro fin, sin previa autorización de la Caja. La violación de tal prohibición tendrá las mismas consecuencias previstas en el párrafo anterior.

La presente cláusula tendrá validez hasta cinco (5) años después de finalizado o entregado el producto o programa objeto de la contratación".

IV. CONSIDERACIONES FINALES

La seguridad de la información es fundamental para mantener la confianza de los ciudadanos respecto a los servicios que brinda la Caja Costarricense de Seguro Social, por lo tanto, un adecuado sistema de control de acceso refuerza la percepción de seguridad y responsabilidad de la institución. Asimismo, fortalecer los mecanismos de control no solo garantizan la protección de la información confidencial, sino que también asegura el cumplimiento legal, previene fraudes y reduce costos a largo plazo.

Es relevante que, los lineamientos de control implementados por la administración activa, definan con claridad cómo se debe clasificar, gestionar y resguardar toda aquella documentación que en la fase de ejecución contractual contenga información y otros datos que no deberían ser de conocimiento general debido a los riesgos que conllevaría su posible exposición o mal uso, lo anterior, sin dejar de lado el cumplimiento de los requisitos de completitud y oportunidad en el registro de la documentación que sí debe constar en el expediente de compra, conforme a lo establecido en la Ley General de Contratación Pública, su reglamento y normativa interna institucional.

Por otra parte, es importante señalar la discrecionalidad que debe de existir en el manejo de los datos generados como resultado de los servicios brindados por la empresa contratada, lo cual, implica que los datos deben ser gestionados con la máxima confidencialidad y asegurando que solo el personal autorizado tenga acceso a ellos y que se utilicen exclusivamente para los fines establecidos en el contrato.

La revisión y análisis de algunos de los documentos que conforman el procedimiento de contratación 2022LN-000003-0001101150 “Servicios para la gestión del Centro de Operaciones de Seguridad (SOC - Security Operation Center)”, ha permitido identificar el riesgo de acceso público y descarga de información que según lo consignado por el proveedor, podría catalogarse como sensibles o de acceso restringido en la citada ejecución contractual, lo que podría generar implicaciones como: exposición de datos, daño a la reputación institucional, así como, posibles sanciones administrativas o legales.

La situación señalada, podría requerir por parte de la Administración Activa de un análisis técnico y legal, para definir posibles vulnerabilidades o incumplimientos contractuales en los procesos de entrega, comunicación, utilización, registro y resguardo de la documentación (física o digital) generada, hasta la fecha, en la etapa de ejecución contractual de la Licitación Pública Nacional 2022LN-000003-0001101150, lo anterior, con el fin de adoptar las acciones que correspondan para garantizar el principio de legalidad y la protección de información sensible para la institución.

De conformidad con lo expuesto, se advierte a esa Administración Activa sobre las debilidades identificadas en relación con el acceso público a documentación que, según lo consignado por el proveedor, podría catalogarse como confidencial o sensible, debido a los riesgos de exposición o mal uso de los datos contenidos en ellos, a fin de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias para garantizar razonablemente el cumplimiento normativo, así como, la integridad, disponibilidad, confiabilidad, calidad y seguridad de la información crítica institucional.

De lo anterior, informar -en el plazo de 1 mes- a esta Auditoría sobre las acciones ejecutadas en atención de lo descrito.

Atentamente,

AUDITORÍA INTERNA

Firmado Digitalmente

M. S.c. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AEBB/ayms

C. Auditoría

Referencia-ID-134488