



AS-AATIC-102-2022

21 de junio de 2022

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA -2901

Máster
Idannia Mata Serrano, subgerente a.i
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Máster
Manuel Rodríguez Arce, director
DIRECCIÓN EXPEDIENTE DIGITAL ÚNICO EN SALUD -4405

Estimados señores:

ASUNTO: Oficio de Asesoría en torno a los equipos tecnológicos utilizados para el Expediente Digital Único en Salud (EDUS) como parte de los contratos de servicios administrados suscritos entre la Caja Costarricense de Seguro Social (CCSS) y el Instituto Costarricense de Electricidad (ICE), afectados por el ciberataque del 31 de mayo del 2022.

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y consecuente al oficio AI-874-2022 del 6 de junio del 2022 en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022, emite la siguiente asesoría sobre aspectos relacionados con los equipos tecnológicos utilizados para el Expediente Digital Único en Salud (EDUS), como parte del equipamiento efectuado a través de los contratos de servicios administrados suscritos entre la Caja Costarricense de Seguro Social (CCSS) y el Instituto Costarricense de Electricidad (ICE).

ANTECEDENTES

Contrato 2013000081: Contrato de venta de servicios entre el Instituto Costarricense de Electricidad y la Caja Costarricense de Seguro Social.

Mediante artículo 26º de la sesión N° 8683, del 5 de diciembre de 2013, la Junta Directiva acordó "(...) adjudicar y autorizar la firma del contrato de servicios administrados para el equipamiento del Proyecto Expediente Digital Único en Salud (EDUS), a favor del Instituto Costarricense de Electricidad por US\$30 792 780,00 (treinta millones setecientos noventa y dos mil setecientos ochenta dólares) (...)".



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: auditoria_interna@ccss.sa.cr

A partir de lo anterior, el 20 de diciembre del 2013, la Arq. Gabriela Murillo Jenkins, Gerente de Infraestructura y Tecnologías en ese momento, firmó el contrato 2013000081, “*Contrato de venta de Servicios entre el Instituto Costarricense de Electricidad y la Caja Costarricense de Seguro Social*”, dando inicio al proceso de implementación de infraestructura tecnológica para el EDUS en el I Nivel de Atención.

En este sentido, el objeto contractual consiste en brindar una solución de servicio administrado para el acceso e interacción con la aplicación del Expediente Digital Único en Salud (EDUS) en los sitios físicos de atención médica, los cuales contemplaban un mínimo de 3600 usuarios, pudiéndose agregar usuarios adicionales por medio de adenda correspondiente entre las partes. Asimismo, la estimación económica del contrato fue de \$30.793.500,00USD (treinta millones setecientos noventa y tres mil quinientos dólares americanos) y el plazo establecido fue de 93 meses.

Sobre este contrato es importante mencionar que en el artículo 17 de la sesión 9208, celebrada el 16 de setiembre de 2021, la Junta Directiva de la Caja en acuerdo tercero, autorizó a la Gerencia Infraestructura y Tecnologías para realizar las gestiones para la prórroga por 60 meses, por tanto, mediante resolución GIT-1387-2021, de fecha 27 de setiembre de 2021, suscrita por el Ing. Jorge Granados Soto, Gerente de Infraestructura y Tecnologías, se autorizó la prórroga del contrato N° 2013000081, Contrato de Venta de Servicios entre el Instituto Costarricense de Electricidad y la Caja Costarricense de Seguro Social, por el plazo adicional de 60 meses de operación, mismo que rige a partir del 01 de diciembre de 2021, con un costo mensual por puesto de trabajo de USD\$ 92 (noventa y dos dólares exactos) por concepto de administración de la red de área local, así como el costo mensual de USD\$24,5 (veinticuatro dólares cincuenta centavos) por concepto de climatización en los sitios en los que aplique (según Oferta Técnico Comercial No. 48-2020, No. 10-2021 y oficio de aclaraciones 9058-1246-2021 del ICE).

En ese sentido, entre las cláusulas modificadas para la prórroga se pueden mencionar las siguientes:

“CLÁUSULA TERCERA: RESPONSABILIDADES DE LA CAJA

La CAJA se compromete a lo siguiente:

(...)

3.2. Realizar en conjunto con el ICE el plan de renovación de elementos en un plazo máximo de 2 meses posterior a la firma de la presente adenda, donde establezca el cronograma de implementación del servicio, el cual define las fechas de realización de las visitas a la totalidad de puestos de trabajo según necesidad, los tiempos instalación, de entrega, y puesta en operación del servicio, así como los roles y responsabilidades de los actores de las partes, de conformidad con el presente Contrato.

3.3. Aprobar el plan de renovación de elementos en un plazo máximo de 5 días hábiles posteriores a la fecha de entrega por parte del ICE.

3.4. Proveer al ICE durante el proceso de elaboración del plan de renovación de elementos a elaborarse entre las partes, el detalle de todas las instalaciones y oficinas donde se requieran brindar los servicios administrados objeto del presente Contrato, aportando para ello su dirección exacta, teléfono, horario y el contacto en sitio (ver anexo 1).



3.5. Proveer al ICE durante el proceso de elaboración del plan de renovación de elementos a elaborarse entre las partes, toda la información técnica, legal, de infraestructura y otras tales como políticas, normas y perfiles, entre otros, que se consideren necesarias para el adecuado dimensionamiento, instalación y configuración de la solución administrada contratada.

(...)

“CLÁUSULA CUARTA: OBLIGACIONES DEL ICE

El ICE se compromete a:

4.1 Brindar a la CAJA una solución de Servicio Administrado integral para ser implementada para un máximo de 3600 usuarios que requieren acceso a la aplicación Expediente Digital Único en Salud (EDUS). Dicha solución involucra la renovación de los elementos necesarios para la correcta operación del acceso al servicio, según lo establecido en Oferta Técnico Comercial No. 48-2020, No. 10-2021 y oficio de aclaraciones 9058-1246-2021 presentadas por el ICE y aceptadas por la CAJA.

4.2 Brindar a partir de la firma de la presente adenda para cada sitio, al menos dos veces al año los servicios de mantenimiento preventivo necesarios para otorgar el Servicio Administrado a la CAJA; todo lo anterior en los sitios acordados, de conformidad con el presente Contrato. Para ello, el cliente debe garantizar el acceso a sus instalaciones para realizar el mismo. En caso de no realizarse por razones atribuibles a la CAJA, y el ICE se encuentre en el sitio se aplicará lo establecido en la Cláusula Decima Novena.

4.3 Realizar en conjunto con la CAJA el plan de renovación de los elementos del servicio administrado en un plazo máximo de dos meses posterior a la firma de la presente adenda, donde establezca el cronograma de renovación de los elementos del servicio, el cual defina las fechas de realización de las visitas a la totalidad de puestos de trabajo según necesidad, los tiempos instalación, de entrega, y puesta en operación del servicio, así como los roles y responsabilidades de los actores de las partes, de conformidad con el presente Contrato.

CLÁUSULA QUINTA: INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DEL SERVICIO

(...)

5.2. Ambas partes deberán desarrollar y aprobar el plan de renovación de los elementos que componen el servicio administrado de conformidad con lo establecido en el presente contrato y la Oferta Técnico Comercial No.48-2020, No.10-2021 y oficio de aclaraciones 9058-1246-2021 para lo cual existirá un plazo máximo de dos meses a partir de la firma de la presente adenda.

(...)

5.6. La solución se ofrece instalada en todos los sitios de la CAJA indicados en el Anexo 1 del presente Contrato, según el orden y prioridad indicada en el plan de renovación de elementos y en las condiciones pactadas.

5.7. El ICE, en todas las visitas que requiera realizar a las instalaciones de la CAJA con motivo de la renovación de los elementos del servicio y la prestación de éste, deberá cumplir con lo indicado en la Cláusula Novena del presente Contrato.



5.8. El ICE comunicará por escrito a la CAJA la finalización de la renovación de los elementos del servicio en cada sitio, para que de acuerdo con la fecha establecida en el cronograma del plan de renovación de elementos se realicen las pruebas de aceptación.

“CLÁUSULA CUARTA: Se modifica la cláusula sexta del contrato original, denominada “TIEMPO DE INSTALACIÓN Y EJECUCIÓN DEL SERVICIO” para que en adelante se lea:

6.1. El periodo máximo de renovación de los elementos del servicio en la totalidad de los sitios contratados es de dieciocho (18) meses contados a partir del 01 de diciembre de 2021. Dicho período comprende el plazo dos (2) meses de planificación para la renovación de los elementos.

6.2. Debido a que el presente corresponde a un servicio continuo, el plazo de operación del servicio de sesenta (60) meses por sitio se tendrá por iniciado en una única fecha, a saber, el 1 de diciembre de 2021 para todos los sitios.”

6.1. El periodo máximo de renovación de los elementos del servicio en la totalidad de los sitios contratados es de dieciocho (18) meses contados a partir del 01 de diciembre de 2021. Dicho período comprende el plazo dos (2) meses de planificación para la renovación de los elementos.

6.2. Debido a que el presente corresponde a un servicio continuo, el plazo de operación del servicio de sesenta (60) meses por sitio se tendrá por iniciado en una única fecha, a saber, el 1 de diciembre de 2021 para todos los sitios.

“CLÁUSULA OCTAVA: DISEÑO DE LA SOLUCIÓN:

(...)

8.11. Los PC se instalan configurados con el sistema operativo de Windows más reciente soportado por el fabricante del hardware al momento de la instalación únicamente e integrados a la red. El servicio incluye la dotación de paquetes de servicios que incluyen terminales que deben estar configurados e integrados a la red para brindar acceso y posibilidad de interacción al EDUS. No se incluye la instalación o soporte para cualquier otro uso, esto incluye la instalación de software adicional, mal uso del terminal o software malicioso (virus).”

Contrato 2017000119, Contrato de venta de Servicios Administrados entre el Instituto Costarricense de Electricidad y la Caja Costarricense del Seguro Social

En el artículo 20 de la sesión No. 8939 celebrada el 16 de noviembre de 2017, la Junta Directiva de la CCSS adjudicó al ICE la compra directa No. 2017CD-000010-1107 “Servicio Administrado para la implementación del Expediente Digital Único en Salud en el nivel hospitalario”, acto que fue ratificado posteriormente en el artículo 22 de la sesión No. 8943, celebrada el 30 de noviembre de 2017.

Así mismo, el 21 de diciembre del 2017, la CCSS y el ICE suscriben el contrato No. 2017000119 con el propósito de brindar a la Institución el servicio administrado de comunicación de datos, mediante una red LAN/WLAN para 29 campus hospitalarios propiedad de la CCSS, bajo la modalidad de entrega según demanda.



La cuantía estimada fue de \$201.000.000,00USD (Doscientos un millón de dólares) por un plazo de 111 meses, es decir 9 años y tres meses y su ejecución inició en enero 2018.

Es importante mencionar que, para otorgar los servicios administrados a la institución, el ICE ha contado con la participación de al menos un “empresario comercial”, quien, según se indica en el contrato, aporta elementos complementarios que son combinados con los servicios que brinda ese ente público.

De conformidad con la cláusula primera, el servicio administrado objeto del contrato contempla los siguientes componentes:

“(...) 1.2.1 Habilitación inicial del servicio de comunicación de datos, cuyo alcance para la interacción de la comunicación EDUS, para lo cual se habilitará una red WLAN, utilizando para ello la infraestructura disponible con la red, con la cual cuenta el sitio. Este componente comprende los servicios descritos en el inciso 1.2.4 del presente Contrato.

1.2.2 Habilitación definitiva del servicio de diseño y construcción de infraestructura de telecomunicaciones, electromecánica y cualquier otra necesaria para la habilitación del servicio, que permitan la conectividad y administración de la red LAN y WLAN, así como el monitoreo, climatización y respaldo eléctrico necesarios para brindar el acceso e interacción a la aplicación de EDUS pero sin limitarse a ella, con capacidad disponible para el transporte de datos del Cliente, todo de acuerdo a los términos regulados el presente Contrato. Este componente comprende los servicios descritos en el inciso 1.2.3 del presente Contrato.

1.2.3 Servicios de transferencia de conocimiento, asesoría y consultoría en servicios eléctricos de telecomunicaciones, infocomunicaciones y otros en convergencia; cuyo alcance está relacionado con el objeto del presente Contrato.

1.2.4 Servicios transversales de operación que incluye: ingenierías, mantenimiento correctivo, mantenimiento preventivo y monitoreo del servicio administrado...”

OBSERVACIONES

Como es ya conocido, la Caja Costarricense de Seguro Social, recibió ciberataques lo cual obligó a desactivar todos los sistemas informáticos de la Institución de manera preventiva.

Debido a lo anterior, esta Auditoría tiene conocimiento que en el transcurso de la emergencia institucional, se han identificado equipos de cómputo que se encuentran encriptados y/o comprometidos en cuanto a su funcionamiento y la disponibilidad de la información, razón por lo cual, entre las directrices emitidas por la Dirección de Tecnologías de Información y Comunicaciones, se encuentra la Guía “*Limpieza de PC infectados del usuario final*”, misma que indica como primer paso una instalación (formateo) del sistema operativo, así como, la aplicación de otras herramientas tendientes a proteger el equipo y restablecer su funcionamiento.



Ante este panorama y tomando en consideración que existen equipos de cómputo afectados en los establecimientos de salud del I, II y III nivel de atención utilizados para el EDUS y forman parte del aprovisionamiento mediante los contratos de servicios administrados señalados en el presente oficio, esta Auditoría establece una serie de observaciones a la Administración Activa, con el objetivo de que sean valoradas como parte de las estrategias y acciones tendientes a restablecer la prestación de servicios que se realiza a través de herramientas informáticas en el contexto del Expediente Digital Único en Salud. A continuación, el detalle:

- Es significativo establecer mecanismos de coordinación y control entre Dirección EDUS, DTIC, Gerencia Médica y sus Centros de Gestión Informática, para identificar la totalidad exacta de equipos de cómputo comprometidos por el ciberataque del 31 de mayo de 2022 y pertenecientes a cada uno de los contratos de servicios administrados suscritos con el ICE, lo anterior en aras de cuantificar el impacto y afectación desde la perspectiva que brinda esta solución de servicio.
- Es pertinente que la Administración Activa valore someter a revisión las cláusulas estipuladas en los contratos en mención, de forma que se logren identificar mecanismos o estrategias que permitan a la Institución dentro del marco de legalidad, obtener un apoyo por parte del ICE a través de sus proveedores y que permitan brindar apoyo a los centros de gestión informática para el eventual formateo de los equipos en caso de ser requeridos, principalmente en el nivel hospitalario, lo anterior en estrecha coordinación con los administradores de contrato e implementando los mecanismos de control que se estimen necesarios como parte de la ejecución contractual.
- En noviembre del 2021, se suscribió una adenda al **Contrato 2013000081**, el cual contempla dentro de los servicios, la dotación de equipos de cómputo para el I nivel de atención, además, entre las cláusulas se establece la obligación de la Caja en conjunto con el ICE de establecer un plan de renovación de los puestos de trabajo, según necesidad, tiempos de instalación, entrega y puesta en operación del servicio, lo anterior en un período máximo de renovación de la totalidad de sitios de 18 meses contados a partir del 1° de diciembre de 2021, el cual comprende un plazo de dos meses de planificación para la renovación de los elementos, los cuales se entregan configurados con el sistema operativo de Microsoft Windows más reciente soportado por el fabricante de hardware al momento de la instalación.
- Considerando lo descrito en el punto anterior, el plan de renovación debió efectuarse entre diciembre 2021 y enero 2022 y el inicio de su ejecución en febrero del presente año. Ahora bien, en el contexto de la declaratoria de emergencia emitida por la Institución a raíz del ataque cibernético y la posible afectación a equipos de cómputo pertenecientes al contrato 2013000081, esta Auditoría estima pertinente que la Administración Activa en conjunto con el ICE y dentro del marco de legalidad que ampara los contratos de servicios administrados, con la aplicación de los mecanismos de control pertinentes y la debida gestión de cambio que resulte necesaria dentro de la ejecución contractual, valore la posibilidad de efectuar una modificación al plan de renovación de los equipos de cómputo, analizando si debe existir prioridad en las estaciones de trabajo que se encuentra comprometidas.
- En ese orden de ideas, una eventual modificación de ese plan posibilita sustituir esas computadoras encriptadas por equipos nuevos, aspecto que podría coadyuvar a los centros de gestión informática del primer nivel de atención en el proceso de limpieza de los PC infectados, generando una mayor cantidad de estaciones de trabajo disponibles para el momento en que se restablezca el Expediente Digital Único en Salud.



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: auditoria_interna@ccss.sa.cr

En virtud de lo esbozado en el presente oficio, de la manera más atenta, este Órgano de Fiscalización y Control hace las observaciones sobre el tema de marras, con el propósito de que en apego a las posibilidades y marco regulatorio aplicable, esa estimable administración valore y analice los aspectos señalados y de ser procedente, establezca las acciones necesarias para su atención, considerando la coordinación con las instancias correspondientes, con el fin de coadyuvar en la mejora de los procesos de trabajo tendientes a restablecer la prestación de servicios con apoyo de los equipos de cómputo y sistemas institucionales.

Finalmente, es relevante manifestar que esta Auditoría se encuentra en la mayor disposición de apoyar la gestión que desarrolle esa Administración ante la temática expuesta, conforme nuestras potestades y competencias.

Atentamente,

AUDITORÍA INTERNA

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/EZCh/lbc

- C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva -1102
Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100
Auditoría