



Al contestar refiérase a: **ID-104223**

AD-ATIC-0134-2023

23 de noviembre de 2023

Máster

Marta Eugenia Esquivel Rodríguez, presidente ejecutiva con cargo de gerente, coordinadora

Consejo Tecnológico

GERENCIA GENERAL-1100

Doctor

Wilburg Díaz Cruz, gerente a.i.

GERENCIA MÉDICA-2901

Máster

Robert Picado Mora, subgerente

DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimados(a) señores(a):

ASUNTO: Oficio de Advertencia referente a la disponibilidad y funcionamiento de los servicios brindados mediante los aplicativos del Expediente Digital Único en Salud (EDUS).

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2023 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, procede a pronunciarse respecto a la disponibilidad y funcionamiento de los servicios brindados mediante los aplicativos del Expediente Digital Único en Salud (EDUS).

I. ANTECEDENTES

I.I La Unión Médica Nacional (UMN) efectuó declaraciones ante la Asamblea Legislativa, referente a distintas problemáticas generadas en el EDUS

Esta Auditoría en el año 2021, tuvo conocimiento respecto a las declaraciones efectuadas por la Unión Médica Nacional (UMN) ante la Asamblea Legislativa, referente a distintas problemáticas generadas (en ese momento) en el Expediente Digital Único en Salud (EDUS).

Al respecto, en medios de comunicación masiva a nivel nacional, se emitieron comentarios y noticias respecto a este tema, respecto a las declaraciones emitidas por Janisse Sandí, vicepresidenta de la Unión Médica Nacional ante la Asamblea Legislativa, en donde se indicó, entre otras cosas, que: “cuando se produce una falla del internet los médicos quedan a ciegas”, “las falencias del EDUS no solo ponen en riesgo la atención de los pacientes sino el trabajo de los médicos”, “hay vulnerabilidades de seguridad en el tema de la firma digital” y que “se le está exigiendo a los médicos atender a más pacientes en el mismo tiempo ante las crecientes listas de espera”.

Asimismo, se señalaron en su momento aspectos como: “No hay un sistema de contingencia en caso de fallo para que no afecte la atención médica” y “la plataforma presenta problemas como duplicidad de recetas, lo que podría provocar que los pacientes tengan sobredosis. Ya se tiene conocimiento de casos en los que usuarios diabéticos tuvieron afectación por esto”.

I.I.I Sobre oficio emitido por la Auditoría y dirigido a la administración activa, en relación con las declaraciones efectuadas por la UMN ante la Asamblea Legislativa

Mediante oficio AI-1472-2021 del 13 de julio de 2021, esta Auditoría informó y solicitó al Doctor Mario Ruíz Cubillo, Gerente Médico y Coordinador Comité Estratégico EDUS-ARCA, al Ingeniero Roberto Blanco Topping, subgerente Dirección de Tecnologías de Información y Comunicaciones y al Ingeniero Manuel Rodríguez Arce, director EDUS, lo siguiente:

“(...) este Órgano de Fiscalización considera necesario revisar y otorgar atención a los aspectos mencionados por la UMN en las declaraciones brindadas, de los cuales se transcriben los siguientes:

- *El expediente en ocasiones no reconoce pacientes nuevos y no hace diferencia del paciente nuevo al subsecuente (...)*
- *Nada de los registros del expediente anterior se ha digitalizado o prácticamente nada. Sería necesario que se contrate médicos para que digitalicen, un médico sabría como resumir un expediente.*
- *Se ha pedido de todas las maneras posibles brindar la firma digital a los funcionarios para acceder al Expediente Digital Único en Salud.*
- *Cuando el sistema está fallando, o no hay conexión de red, en el caso se esté digitando una nota médica, al dar la indicación de guardar esa información, no queda registrada.*
- *Si el internet se cae, no hay acceso al Expediente digital. Si bien se habla de una herramienta que guardaba la última información en los nodos más cercanos al centro de salud, eso no existe, ese backup no funciona. No se dispone de respaldo que permita tener acceso a las notas registradas los últimos cinco días en caso de presentarse una emergencia de este nivel.*
- *En la Consulta Externa, como la agenda ya está programada, entonces si hay interrupción del sistema o de la red, no existe forma de ir incluyendo la nota médica y acceder a la última información registrada del expediente de los pacientes citados en ese periodo de tiempo.*
- *Cuando hacen un pase a producción, el 99% de las veces hay problemas con los sistemas, hay que reportar incidencias a la mesa central con un número de teléfono donde no atienden oportunamente.*
- *Para este tema se ha solicitado que en el App del EDUS, se habilite un acceso exclusivo para el personal donde se pueda reportar en una forma automática e inmediata lo que está pasando (...)*
- *No existe una alerta de despacho en medicamentos similares en el sistema SIFA (Sistema de Farmacia) en forma integrada para todos los centros de atención.*
- *El sistema SIFA no tiene trazabilidad en relación al despacho o no de un medicamento suspendido en cualquier lugar del País.*
- *El sistema de Receta digital no está respaldado por una firma digital (...)*

(...) Se requiere que la Gerencia Médica en su función de rectoría institucional en materia de prestación de servicios de salud, así como su rol de coordinación del Comité Estratégico EDUS-ARCA, así como la Dirección EDUS y la Dirección de Tecnologías de Información y Comunicaciones, cada una en su posición táctica dentro de la CCSS y participación en la implementación y uso de tecnologías relacionadas con el Expediente Digital Único en Salud (EDUS), brinden la siguiente información de acuerdo con los temas mencionados anteriormente (...)”

Asimismo, ante la ausencia de la totalidad de la información, solicitada mediante el oficio AI-1472-2021, esta Auditoría en oficio AI-2107-2021 del 1 de octubre de 2021 reiteró a las unidades citadas anteriormente, los datos requeridos.

De conformidad con lo anteriormente mencionado y ante la carencia aún existente, de la información solicitada por este Órgano de Fiscalización, mediante oficio AI-2439-2021 del 18 de noviembre de 2021, se solicitó al Dr. Roberto Cervantes Barrantes, Gerente General en ese momento, su intervención para que el requerimiento de este Órgano de Fiscalización y Control, fuera atendido según los términos indicados en el oficio AI-1472- 2021 del 13 de julio del 2021 y reiterado en el AI-2107-2021 del 1 de octubre del 2021.

I.II El Sindicato Unión Médica Nacional comunicó, nuevamente, algunos riesgos evidenciados en funcionamiento del Expediente Digital Único en Salud.

Mediante oficio UMN-0458-2022 del 07 de diciembre de 2022, el Sindicato Unión Médica Nacional comunicó a la Junta Directiva, algunos puntos críticos respecto al manejo del Expediente Digital Único en Salud, señalando lo siguiente:

“(...) Para su conocimiento les señalamos algunos de los puntos críticos respecto al manejo del Expediente Digital Único en Salud que consideramos deben ser tomados en cuenta por ustedes como máximos jerarcas de la Institución:

1. No se ha generado una plataforma amigable que permita conocer en tiempo real las situaciones de fallo que ocurren a nivel nacional. Por tanto, toda esta cadena de errores es desconocida por quienes deben tomar decisiones y mejorar la atención técnica que se merece el expediente digital.

2. Desde antes del hackeo hemos insistido en mantener un canal de dialogo entre Unión Medica Nacional y los grupos que lideran la implementación y soporte técnico del EDUS. Sin embargo, desde hace más de un año no ha sido posible generar estos encuentros ante la cancelación reiterada de los mismos por parte de los funcionarios encargados en la CCSS.

3. Pese a que hemos insistido ante la Gerencia General y la Gerencia Médica la institución no ha logrado generar un Protocolo Institucional de Accionar en caso de caídas mayores a 15 minutos dejando a cada unidad a su suerte sin la directriz gerencial, poniendo en alto riesgo médico legal tanto a la Institución como a los colegas visto que en aquellas unidades en las que se pasa a atención manual utilizando, en la mayoría de las ocasiones, hojas sueltas de evolución.

4. *Tampoco existe algún sistema de respaldo para garantizar que, en caso de fallo del sistema, al menos se tengan últimas notas consignadas en el expediente digital. Esto pone en riesgo, en especial, a los pacientes que se encuentran ingresados en nuestros hospitales con condiciones clínicas agudas.*

Con responsabilidad y estoicismo el cuerpo médico nacional le hizo frente a la emergencia generada por un hackeo en el que medió una enorme falta de ciberseguridad por parte de la Institución, tal como fue denunciado en su momento por Unión Médica Nacional. Nosotros estamos totalmente de acuerdo en que la digitalización completa del expediente clínico debe ser el norte del accionar de la Caja Costarricense de Seguro Social pero, con gran desazón y pese a la gravísima experiencia sufrida durante el ciberataque, vemos que no se ha logrado integrar un equipo de profesionales en informática que, en conjunto con profesionales del área clínica, brinden herramientas con alto grado de seguridad y que permitan mantener un contexto de funcionalidad acorde con el complejo quehacer clínico dentro de la Institución.

Por todo lo expuesto les solicitamos consideren realizar una investigación de lo aquí expuesto y una intervención directa, desde Junta Directiva, para asegurar que la atención clínica de nuestros asegurados no sea obstruida por las graves falencias informáticas y de procedimiento que, con todo respeto, hemos señalado ante ustedes”.

Mediante oficio TDI-JD-0280-2022 del 09 de diciembre de 2022, con instrucciones de la Ing. Carolina Arguedas Vargas, jefe de Secretaría Junta Directiva se traslada el documento UMN-0458-2022 a la Gerencia Médica, para su atención y resolución.

De conformidad con la información anteriormente señalada, mediante oficio AI-2033-2023 del 18 de octubre de 2023, esta auditoría solicitó a la MSc. Marta Eugenia Esquivel Rodríguez, presidente ejecutiva con cargo de gerente, coordinadora Consejo Tecnológico y al Dr. Wilburg Díaz Cruz, gerente médico a. i., brindar información respecto a las gestiones efectuadas para dar atención a los aspectos señalados por representantes de la Unión Médica Nacional (UMN) sobre problemas en la disponibilidad y funcionamiento del EDUS.

En respuesta a la solicitud anterior, mediante oficio GM-15668-2023 del 24 de octubre de 2023, el Dr. Wilburg Díaz Cruz, gerente médico a. i, informó a esta auditoría, lo siguiente:

“(…) me permito comunicar que mediante oficio GM-12244-2023 del 04 de septiembre de 2023 este Despacho quedó atento a las consideraciones de la Presidencia Ejecutiva para la atención del informe ATIC-129-2022 y así poder atender los aspectos señalados tanto por la Unión Médica Nacional (UMN) como por este Órgano Fiscalizador”.

Como complemento de la información anteriormente citada, el Dr. Wilburg Díaz Cruz, gerente médico a. i, remitió a este Órgano de Control y Fiscalización el oficio GM-16626-2023 del 09 de noviembre de 2023, donde comunicó las acciones realizadas por la Gerencia Médica para la atención de cada uno de los oficios citados en el oficio AI-2033-2023 del 18 de octubre de 2023, indicando lo siguiente:

“(…) me permito informar a ese Órgano de Control y Fiscalización las acciones realizadas por este Despacho para la atención de cada uno de los oficios citados en dicha misiva:

AI-1472-2021: Se realizó oficio GM-11248-2021 a la Dra. Priscilla Balmaceda Chaves, Coordinadora en ese momento del Comité Gestor EDUS-ARCA, la cual da respuesta mediante oficio CE-EDUS-ARCA-0093-2021 y el cual fue trasladado mediante misiva GM-14646-2021 del 22 de octubre de 2021 a esa Auditoría Interna, en el cual indican lo siguiente:

“(...) se remite el oficio CE-EDUS-ARCA-0093-2021 de fecha 21 de setiembre del 2021, en el cual la Dra. Priscilla Balmaceda Chaves, Coordinadora del COMITÉ GESTOR EDUS-ARCA, informa que mediante oficio CE-EDUS-ARCA-0083-2021 del 20 de setiembre del 2021, se remitió la información requerida al Despacho a su cargo. (...)”.

AI-2107-2021: En atención a dicho oficio este Despacho solicitó al Comité Gestor EDUSARCA, remitir la información requerida, relacionada con cada aspecto señalado en el oficio AI-1472-2021, por lo cual se remite el documento CE-EDUS-ARCA-0106-2021 de fecha 05 de noviembre de 2021, suscrito por el Dr. Eduardo Rodríguez Cubillo, Coordinador del Comité Gestor EDUS ARCA, en el cual da respuesta concreta y se trasladó a ese Órgano Fiscalizador en oficio GM-0600-2022.

UMN-0458-2022: Oficio de la Unión Médica Nacional (UMN) el cual fue enviado a los Señores Junta Directiva, con copia a este Despacho, se realizaron las acciones correspondientes mediante las siguientes misivas:

GM-2046-2023 (copia en su poder) del 14 de febrero del 2023, se dio respuesta al Dr. Edwin Solano Alfaro, presidente de la Unión Médica Nacional, en el cual se atiende los 4 puntos indicados en dicho oficio, que a la letra indica textuales:

1. (...) Esta Gerencia ha servido a través de diversos canales de comunicación, como mediador entre la Dirección de Tecnología de Información y Comunicaciones, los gestores locales y regionales EDUS en las diferentes áreas del país, durante los momentos de fallos inesperados en los sistemas o redes, transmitiendo la información en tiempo real, para que los diferentes centros y los responsables de la toma de decisiones puedan actuar conforme a los recursos disponibles y capacidad instalada en sus lugares de trabajo, así mismo alertando mediante comunicados en webmaster y consejos de directores cuando estas interrupciones son mantenimientos programados.

En cuanto a la atención técnica, mantenimientos y el monitoreo del estado de red y aplicativos, así como la elaboración y publicación de una herramienta o consola de monitoreo, son acciones que se enmarcan en las competencias de la Dirección de Tecnología Información y Comunicaciones en la Gerencia General. Para lo cual, la Gerencia Médica, en representación de los usuarios gestionará ante la DTIC las acciones necesarias para buscar alternativas o valorar en conjunto la propuesta de generar una plataforma o visualizar en las existentes (mesa de servicios) información de consulta en situaciones de fallos, imprevistos o mantenimientos.

2. (...) En lo que respecta al ciberataque, el día 31 de mayo del 2022, la Caja Costarricense del Seguro Social presentó alerta por hackeo, lo que obligó a desconectar la plataforma tecnológica que incluye los sistemas de información de la institución, entre ellos el Expediente Digital Único de Salud (EDUS).

A partir de ese momento, la institución inició un proceso de sanitización del parque tecnológico, hasta llegar a considerar una seguridad relativa para el levantamiento de los sistemas y retomar el uso de estos, su normalidad.

Durante el año 2022, se tenía programada la participación de la Unión Médica Nacional en el comité Gestor EDUS-ARCA, según la frecuencia acordada en sesión del 13 de diciembre del 2021(...)

Sin embargo, luego de la sesión mantenida con la Gerencia Médica el día 20 de diciembre 2022, por parte de la UMN se acordó mutuamente reanudar estos espacios de diálogo, retomando la primera participación del año 2023 el día 31 de enero del 2023, a las 2:00 pm junto al Comité Gestor EDUS - ARCA.

En cuanto a las sesiones con el Equipo Integrador EDUS – ARCA, se realizó mediante el oficio EIEDUS-003-2022 el cese formal de funciones debido al fortalecimiento y experiencia, de los equipos técnicos a nivel central, quienes asumieron gran parte de los objetivos del Equipo Integrador.

3. (...) *Desde el 2013, se encuentra en vigencia el “Manual para Elaborar un Plan de Continuidad de la Gestión en TIC”, disponible en la intranet de la institución, el cual instruye a las unidades a generar y establecer el accionar ante eventos de contingencia acorde a sus recursos y capacidad instalada (...)*

Mediante oficio EDAC-551-2022, se trasladó para revisión de las instancias técnicas en el Área de Estadística en Salud, el Manual Operativo del Reglamento del EDUS – Continuidad de la Gestión, como complemento a la serie de manuales operativos del Reglamento al Expediente Digital Único en Salud.

Dicho documento pretende establecer los lineamientos, para una adecuada gestión de la continuidad en la prestación de servicios de salud que se desprenden del uso del EDUS, así mismo, contempla las responsabilidades asignadas a los diferentes actores del proceso y las acciones a seguir por parte de las diferentes unidades, como preparación ante una contingencia y las acciones posteriores al restablecimiento de los sistemas.

Importante hay que mencionar que, para la elaboración de este manual, se contó con la colaboración de instancias técnicas de la institución.

4. (...) *En cuanto al EDAC, que en su versión 2.5.11 se encontraba funcionando previo al ciber ataque, luego de las labores de rehabilitación de las plataformas se solicitó el criterio a DTIC sobre la viabilidad de usar nuevamente el EDAC, para determinar si la estructura de funcionamiento no representaba vulnerabilidad y posible amenaza en materializar el riesgo de un hackeo, sin embargo este criterio fue negativo, ya que, se consideró que se requiere mejorar el mecanismo de distribución de los archivos de respaldo o rediseñar el software para lo que es requerido un equipo de desarrollo completo, del cual no se dispone por DTIC, aspecto que ha sido analizado por el Consejo Tecnológico Institucional.*

Para la Gerencia Médica, es urgente el desarrollo de un sistema que permita acceder la información sobre periodos de desconexión de los sistemas, necesidad que también ha sido externada por parte de este despacho. A raíz de esto, se han retomado las coordinaciones con la Dirección de Tecnologías de Información y Comunicación, con el fin de establecer la línea de trabajo para contar con un sistema que, permita visualizar la información clínica de los usuarios, en periodos donde no se cuente con acceso a los sistemas de información (...).

Es importante señalar que, a la fecha de emisión del presente oficio, la Presidencia Ejecutiva en su rol de coordinación del Consejo Tecnológico, no había remitido a esta auditoría, información respecto a las gestiones efectuadas para dar atención a los aspectos señalados por representantes de la Unión Médica Nacional (UMN) referentes al funcionamiento y continuidad del EDUS, solicitada mediante oficio AI-2033-2023 del 18 de octubre de 2023.

I.III Solicitud de intervención urgente, por parte del Sindicato Unión Médica Nacional, debido a problemas que se están presentando en el EDUS

Adicional a los hechos anteriormente expuestos, el 23 de octubre de 2023, mediante oficio UMN-0463-2023 el Sindicato Unión Médica Nacional efectuó un nuevo comunicado, donde solicitó a la Msc. Martha Eugenia Esquivel Rodríguez, presidenta ejecutiva y el Dr. Wilburg Alonso Díaz Cruz, gerente médico a.i, una intervención urgente para establecer un plan de contingencia debido a los problemas que se están presentando en el EDUS, señalando lo siguiente:

*“(...) La Unión Médica Nacional recurre nuevamente ante su autoridad, con el fin de solicitarle su **intervención urgente** para establecer un plan de contingencia en vista de los serios problemas que está enfrentando el EDUS (...) para tal efecto exponemos lo siguiente:*

I.- Antecedentes:

- 1. El día de hoy lunes 23 de octubre, el EDUS nuevamente está presentando lentitud a nivel nacional en cuanto a su funcionamiento. Esta penosa situación ha venido siendo constante en los últimos meses.*
- 2. Los riesgos por el mal funcionamiento del EDUS son tangibles y las consecuencias para la Institución son altamente peligrosas.*
- 3. En este momento se están atendiendo pacientes que presentan emergencias médicas y en estos casos es vital que el Médico tenga acceso inmediato a los estudios de gabinete, exámenes y medicamentos de rigor.*
- 4. Las consultas que no cumplan con todos los parámetros de ley lamentablemente terminan siendo reprogramadas, situación que aumenta las listas de espera y eleva los costos de la institución.*
- 5. Día a día el médico se expone a esta situación, con el agravante de que el paciente lo señala como culpable y ninguna autoridad institución asume su responsabilidad (...)*

III.- Responsabilidad Institucional y petición:

*(...) La lentitud del EDUS y en especial el hecho de que no exista un plan de contingencia claro y preciso que se active de inmediato cuando se presentan estas circunstancias, además del compromiso que esto significa en contra del **acto médico**, son motivos suficientes para acudir ante ustedes y solicitarles lo siguiente:*

A.- Emitir de inmediato un plan de contingencia serio y preciso para disminuir o por lo menos paliar los problemas que provoca el EDUS cuando se retarda, lo cual pone en riesgo el acto médico y altera la relación médico-paciente.

B.- Aclararle a la opinión pública que los problemas que se presentan en el retraso de la atención médica son por causa del EDUS.

C.- En vista de la seriedad del caso, nuestra organización social se reserva la posibilidad de acudir ante cualquier instancia que sea necesaria para advertir, denunciar o aclarar esta situación tan lamentable que expone al cuerpo médico y a los pacientes.

D.- Siendo que no existe un plan de contingencia debidamente elaborado, procederemos a indicarle a los médicos que en estricto cumplimiento del artículo 108 de las Normas que regulan las relaciones entre la CCSS y los médicos, reprogramen las citas correspondientes hasta tanto no obtengamos respuesta de las autoridades institucionales.

E.- Finalmente, no quisiéramos pensar que media algún interés desconocido o con intenciones privatizadoras que esté provocando reiteradamente este enlentecimiento y caída no explicada del expediente digital EDUS, en el cual, dicho sea de paso, la CCSS ha invertido muchísimo presupuesto.

Por lo expuesto, quedamos a la espera de la respuesta, misma que la pedimos bajo el derecho de petición y pronta respuesta según el numeral 27 de nuestra Constitución Política (...)"

I.IV Solicitud de intervención inmediata, por parte de la Gerencia Médica, debido a problemas de funcionamiento y continuidad de los servicios brindados mediante el EDUS

En la misma línea de informar y alertar a las autoridades institucionales, respecto a problemas generados en el funcionamiento y continuidad de los servicios brindados mediante el Expediente Digital único en Salud (EDUS), el Dr. Wilburg Díaz Cruz, Gerente Médico, mediante oficio GM-15606-2023 del 23 de octubre de 2023, informó a la Msc. Martha Eugenia Esquivel Rodríguez, presidenta ejecutiva con recargo de gerente general y coordinadora del Consejo Tecnológico, así como, al MSc. Robert Picado Mora, director de la Dirección de Tecnologías de Información y Comunicaciones, lo siguiente:

"(...) Me permito externarle la preocupación que tiene nuestra Gerencia Médica ante la gran inestabilidad que ha presentado las aplicaciones EDUS, desde hace algunos meses ya, en donde resulta constante los reportes de imposibilidad de utilización, problemas de reportería, problemas de logueo y en fin, diversas situaciones que están provocando una alteración en la oportunidad de la prestación de los servicios de salud a través de los aplicativos, que por demás esta decir hoy en día son pieza fundamental del trabajo diario en todo el país y que al generar retrasos o trabajo contingente de manera constante, no coadyuva en la meta de lograr mayor eficacia y resolutivez en la prestación de servicios de salud.

Especialmente relevante, en todas estas incidencias, el caos de todos los lunes donde, desde primera hora la aplicación esta inaccesible; siendo la retroalimentación recibida por parte de la Dirección de Tecnologías de información y Comunicaciones un elemento susceptible de importante mejora, pues realmente no existe un canal, espacio o grupo de trabajo en donde como Gerencia podamos tener claridad en las causas y podamos coadyuvar en la búsqueda de soluciones.

Muy significativa la incidencia del día de hoy 23 de octubre de 2023, o quizás un poco el desborde de enfrentar de manera continua y por tanto tiempo el mismo asunto sin aparentes soluciones; donde TODO el país reporta caída de los aplicativos EDUS y además sin disponer de retroalimentación, plazo estimado de solución, un plan de mitigación para que esto no pase todos los lunes sin falta, en fin, acciones mínimas de actuación para que nuestros servicios de misión crítica no se vean afectados o en todo caso, para que los establecimientos de salud apliquen sus planes de continuidad con parámetros claros que faculten la gestión de los escasos recursos disponibles en el nivel local. Por demás está decir, que una actuación constante de contingencia no es una práctica saludable en servicios que deberían disponer de un altísimo nivel de disponibilidad de la plataforma tecnológica, al contar de un nivel muy alto de automatización en todos sus extremos.

Aunado a lo anterior, esta Gerencia Médica ha estimado este año 2023 como un hito negativo en el progreso del Expediente Digital Único en Salud, pues se ha mostrado un creciente sentimiento de inviabilidad en todos los campos asociados a los procesos de automatización, existiendo una lentitud en la respuesta de los equipos de desarrollo de software por falta de capacidad instalada, existiendo importantes mejoras requeridas en procesos de adquisición de soluciones de infraestructura tecnológica a nivel nacional que se integren efectivamente a la institución, se perciben dificultades de inversión por parte de la Dirección de Tecnologías de Información y Comunicación para solventar efectiva y definitivamente los problemas de rendimiento y plataforma asociada al EDUS dentro de un entorno de seguridad digital adecuado; en fin desde todos los ámbitos asociados a la enorme complejidad que significa brindar sostenibilidad y garantizar el crecimiento de soluciones de alta complejidad que facultan la automatización de servicios de misión crítica ofrecidos por parte de esta gerencia en beneficio de todos nuestros usuarios (...)

Es importante mencionar el impacto que produce la debilidad de las características claves en el proceso de atención directa, por área de atención:

1. Consulta externa:

- a. Aplicativos afectados de atención directa a los usuarios: SIAC, SIES.*
- b. Retraso en los horarios de atención: Afectación directa a los usuarios que no son atendidos en las horas indicadas, esta ralentización de los sistemas de información ha dado lugar a considerables retrasos en la prestación de servicios de salud. Esta situación afecta la eficiente operativa, y un genera un gran impacto directo en la calidad de la atención.*
- c. Se pone en riesgo el registro, la integridad y completitud de las historias clínicas al verse obligados a implementar el uso de expediente físico.*
- d. No permite el uso de herramientas de consulta de información (Cubos) para toma de decisiones por autoridades.*

2. Emergencias:

- a. *Aplicativos afectados de atención directa a los usuarios: SIUR, SIES.*
- b. *La persistente lentitud de nuestros sistemas de información está generando retrasos significativos en la atención de los servicios de urgencias, lo que pone en grave riesgo la salud de quienes acuden en busca de ayuda. Cada minuto cuenta en situaciones de emergencia, y la demora en el acceso a la información vital puede resultar en consecuencias perjudiciales. Es imperativo que abordemos este problema de manera urgente para garantizar que podamos brindar atención rápida y efectiva a quienes más lo necesitan, salvaguardando así la salud y el bienestar de nuestros pacientes en situaciones críticas.*
- c. *Se pone en riesgo el registro, la integridad y completitud de las historias clínicas al verse obligados a implementar el uso de expediente en físico.*

3. Hospitalización:

- a. *Aplicativos afectados de atención directa a los usuarios: SIES, Arca-Admisión y Egreso y Módulo Quirúrgico.*
- b. *Problemas en la red que ocasiona dificultades con el funcionamiento de los diferentes sistemas, tanto el ingreso y egreso de pacientes, así como el registro de las anotaciones clínicas en el expediente de cada paciente hospitalizado, el seguimiento a tratamiento de dichos pacientes, así como el registro oportuno de anotaciones en general, y sobre las quirúrgicas afectaría su resolución en la lista de espera, entre otras.*
- c. *Problemas en la integración entre SIES y Arca-Admisión y Egreso y Módulo Quirúrgico.*
- d. *Se pone en riesgo el registro, la integridad y completitud de las historias clínicas al verse obligados a implementar el uso de expediente en físico.*

Al respecto y ante la manifestación clara de gran cantidad de riesgos que están alterando de manera muy significativa la prestación de los servicios de salud, apelo a sus buenos oficios para dictaminar una intervención inmediata, pero más importante aún definitiva, para garantizar la estabilidad técnica, presupuestaria, humana y de recursos en general para el proceso de automatización más importante que posee la Institución y pilar fundamental en la prestación de servicios de salud Institucionales. Recordando en este contexto, que el EDUS es la base de todo el proceso de la ruta de salud digital establecido por el Gobierno de la República y bajo el contexto de inestabilidad en que se encuentra en este momento, no solo paraliza y entorpece el quehacer de institucional, sino pone en riesgo ese mismo proceso país pues resultará muy improbable lograr una interoperabilidad adecuada bajo constantes caídas de la plataforma (...)."

I.V Otros documentos relacionados con el funcionamiento de EDUS y EDAC

Mediante oficio GG-DTIC-CISADI-1905-2023 del 30 de octubre de 2023, el Ing. Manuel Rodríguez Arce, coordinador del Componente de Innovación y Salud Digital, informó al MSc. Robert Picado Mora, subgerente Dirección de Tecnologías de Información y Comunicación que, ya que actualmente persiste la necesidad de disponer de un medio de contingencia del EDUS, esta línea de trabajo se incluyó como parte del replanteamiento del PESDI hacia la Madurez Digital de las soluciones EDUS, con el fin de presentar la necesidad de fortalecer recursos ante el Consejo Tecnológico y la Junta Directiva según corresponda.

Respecto a lo externado por el ingeniero Rodríguez Arce en el oficio anterior, es importante tener presente que, mediante oficio SJD-2328-2023 del 09 de noviembre de 2023, la Ing. Beatriz Guzmán Meza, Secretaría de Junta Directiva a.i, comunicó al MSc. Juan Ignacio Monge Vargas, jefe despacho Gerencia General, lo resuelto por la Junta Directiva de la Caja en el artículo 11° de la sesión N° 9383, celebrada el 09 de noviembre de 2023; en la que se acordó brindar un plazo de dos meses (solicitado el Consejo Tecnológico) para que se realice el replanteamiento del PESDI hacia “Ruta de Madurez Digital de las soluciones EDUS”.

Por otra parte, en relación con las posibles fallas del EDUS, mediante oficio GM-15942-2023 / GG-DTIC-7274-2023 del 02 de noviembre de 2023, el Dr. Wilburg Díaz Cruz, gerente médico a.i y el MSc. Robert Picado Mora, subgerente Dirección de Tecnologías de Información y Comunicaciones, remitieron a los directores de hospitales nacionales, especializados, regionales y periféricos; directores de áreas de salud y a los jefes de CGI gerenciales, de hospitales y de áreas de salud, un recordatorio sobre la necesidad de que las unidades revisen actualice e implementen los Planes de continuidad ante posibles fallas del EDUS.

II. PRODUCTOS DE AUDITORIA RELACIONADOS

En los últimos años, debido al aumento significativo en la utilización de sistemas información para los procesos de atención directa a los usuarios de los servicios de salud institucionales, así como, el ciberataque contra los servidores de la C.C.S.S, ocurrido el 31 de mayo de 2022, esta auditoria ha emitido diversos productos orientados al fortalecimiento de los mecanismos de control, ciberseguridad, planes de continuidad tic, estrategias de recuperación, continuidad del negocio, gestión de crisis, medidas de contingencia, entre otros; los cuales, podrían ser utilizados por la administración activa como insumos para el análisis y toma de decisiones, en torno a las actividades que se deben efectuar para la atención de los hechos señalados por el Sindicato de la Unión Médica Nacional y la Gerencia Médica de nuestra institución, respecto los problemas de funcionamiento, disponibilidad y contingencia del EDUS.

En el Anexo 1, se señalan algunos de estos informes de control interno y oficios de asesoría o advertencia, y se transcribe (de manera resumida) aspectos comunicados a la administración activa, en su momento, para su respectiva atención.

III. CONSIDERACIONES NORMATIVAS.

La Ley Expediente Digital Único en Salud, No.9262, en el artículo 5, sobre la orientación de la solución tecnológica, señala:

“(...) La solución tecnológica deberá contener, al menos, las siguientes características claves:

a) Interoperabilidad: las aplicaciones, los equipos y los servicios que interactúen con el expediente digital único de salud deberán disponer de las capacidades necesarias para garantizar un intercambio de información efectivo de forma transparente, de acuerdo con los parámetros que para tales efectos establezca la Caja Costarricense de Seguro Social.

b) *Mejores prácticas: las soluciones tecnológicas que conformen el expediente digital deberán diseñarse y operar tomando como referencia las mejores prácticas, tanto en los procesos de atención médica como en el campo de las tecnologías de información y comunicaciones. Se deberá prestar especial énfasis en la incorporación de protocolos de medicina basada en la evidencia y guías de atención médica.*

c) *Seguridad: el expediente digital y las soluciones informáticas que interactúen con este deberán cumplir los criterios que para tal efecto se establezcan en los ámbitos tecnológico, científico, ético y administrativo, en aras de garantizar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos contenidos en el expediente clínico.*

d) *Escalabilidad: la solución informática deberá poseer una arquitectura que permita hacer frente, de forma gradual, al incremento en el número de usuarios, peticiones y nuevos servicios en el expediente digital que se demanden en el futuro.*

e) *Usabilidad: las interfaces de las soluciones que conforman el expediente digital deberán ser diseñadas para tener un aspecto uniforme y amigable, que facilite los procesos de aprendizaje y gestión del cambio en el uso de la herramienta informática, aumentando la productividad en el trabajo y minimizando el riesgo de errores en su operación.*

f) *Productividad y calidad: la solución deberá permitir incrementar la calidad, eficiencia, eficacia y oportunidad en la prestación de los servicios de salud, optimizando la relación entre insumos y productos asociados a dichos servicios, bajo un enfoque de mejora continua.*

g) *Portabilidad: acorde con la estrategia de implementación podrá introducirse la característica de portabilidad de la información contenida en el expediente digital, mediante la cual los usuarios podrán llevar consigo la información esencial de su expediente mediante el uso de dispositivos electrónicos.*

h) *Integridad: la información deberá permanecer sin alteraciones desde su origen, asegurando la calidad y confiabilidad de los datos, en la evolución del proceso salud enfermedad (...)*

i) *Requerimientos para la prestación de servicios de salud: el expediente digital deberá atender los objetivos funcionales y las funcionalidades que requieren los servicios de salud en los tres niveles de atención, incluyendo soluciones informáticas para la implementación de la receta electrónica, la gestión telemática de citas y la imagenología digital, sistema de interconsulta y referencia y contrarreferencia (...)*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señalan:

(...) I. PLANIFICACIÓN TECNOLÓGICA INSTITUCIONAL

La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público (...)

IV. GESTIÓN DE RIESGOS TECNOLÓGICOS

(...) La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución (...)

XI. SEGURIDAD Y CIBERSEGURIDAD

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 (...)”.

XIII. CONTINUIDAD Y DISPONIBILIDAD OPERATIVA DE LOS SERVICIOS TECNOLÓGICOS

La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas (...)”

El Reglamento del Seguro de Salud en el capítulo i “Principios generales y campo de aplicación”, Artículo 5° “De la eficiencia”, se indica:

“La eficiencia se considerará como la mejor utilización social y económica de los recursos administrativos, técnicos y financieros disponibles para que los beneficios a que da derecho el Seguro de Salud sean prestados en forma adecuada, oportuna y eficaz”.

Este mismo marco normativo, en el capítulo VI “Derechos y deberes de los usuarios”, Artículo 75° “De los derechos de los asegurados”, señala:

“Los asegurados tienen derecho a:

a) Ser atendidos en forma oportuna, dentro de las posibilidades de la Institución, con el máximo de respeto, sin discriminación alguna, bajo una relación que destaque su condición de ser humano (...)

c) Que toda la información que genere el sistema de salud sea documentada, sin ningún tipo de exclusión o de excepción, en el expediente clínico (...)

e) *Que todos los informes y registros reciban trato absolutamente confidencial, salvo cuando por ley especial deba darse noticia de ellos a las autoridades sanitarias (...)*

ñ) *Esperar una atención continua, y a recibir información sobre sus necesidades de atención (...)*”

IV. CONSIDERACIONES FINALES

Los servicios de salud que brinda la Caja Costarricense de Seguro Social, desde su creación, son de vital importancia y uno de los pilares esenciales para garantizar el bienestar y desarrollo de la población costarricense, motivo por el cual, ante la necesidad creciente de disponer de tecnologías que contribuyeran con la mejora continua de la atención a los usuarios, fue necesario la creación e implementación del Expediente Digital Único en Salud (EDUS), el cual, se ha convertido en una herramienta con un papel protagónico y de gran orgullo a nivel mundial, debido al avance e impulso tecnológico que le ha brindado a la institución y al sector salud de la región.

No obstante, según la información recopilada por esta auditoría, se observa que en reiteradas ocasiones (de manera más frecuente, en el presente año), diversos entes y unidades institucionales han notificado la existencia de problemas en la disponibilidad y funcionamiento de los servicios brindados mediante los aplicativos del Expediente Digital Único en Salud.

Uno de los aspectos cruciales identificados por esta auditoría, se relaciona con la necesidad imperativa de asegurar la continuidad del funcionamiento del EDUS, sin interrupciones, para preservar la atención médica oportuna y efectiva de los pacientes.

Estos problemas de disponibilidad y funcionamiento podrían generar consecuencias graves, desde retrasos en el acceso a los expedientes médicos, aumento significativo de errores diagnósticos y de prescripción de tratamientos, así como, las posibles repercusiones legales en las que podría incurrir el profesional en salud y la institución ante una inadecuada atención de un paciente.

Por otra parte, no podemos dejar de lado que, la CCSS tiene la responsabilidad funcional y legal de proporcionar una atención médica de calidad a los pacientes y de mantener la oportunidad, disponibilidad y confidencialidad de sus datos médicos.

Si bien es cierto, según la información recopilada por esta auditoría, las autoridades institucionales han ejecutado diversas acciones orientadas a la corrección de debilidades en el funcionamiento del EDUS, también es necesario señalar que, a más de dos años de haberse efectuado las primeras manifestaciones del Sindicato de la Unión Médica Nacional respecto a problemas suscitados en algunos de los aplicativos del EDUS y considerando los riesgos evidenciados ante medios de comunicación masivos, la Asamblea Legislativa y autoridades institucionales; en la actualidad, se continúa informando y advirtiendo de situaciones que además de producir afectación en la continuidad de los servicios, podría repercutir en la oportunidad y calidad de la atención a los usuarios.



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

Para mitigar estos riesgos, es imperativo que las autoridades institucionales en coordinación con las unidades involucradas implementen medidas preventivas y de contingencia para garantizar la disponibilidad y la robustez del Expediente Digital Único en Salud. Para lo cual, como insumo para la toma de decisiones, podrían analizarse aspectos como: implementación de sistemas de respaldo, la planificación de continuidad del negocio, la revisión y mejora de las políticas de gestión de datos, la capacitación del personal para afrontar situaciones de emergencia, así como, la inversión en infraestructura y recursos para mantener la estabilidad de la herramienta tecnológica.

En virtud de lo expuesto, se previene y advierte a esa Administración con el propósito que se adopten las medidas técnicas, administrativas y presupuestarias tendientes a garantizar la disponibilidad, confiabilidad, integridad y seguridad de los servicios brindados mediante los aplicativos del Expediente Digital Único en Salud (EDUS) y la mejora continua de la atención brindada a los usuarios.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada, en el **plazo de 1 mes** a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AEBB/lbc

Anexo(1)

1. Productos de Auditoría respecto a: Ciberseguridad, planes de continuidad tic, estrategias de recuperación, continuidad del negocio, gestión de crisis, medidas de contingencia, EDUS y EDAC.

C.Auditoría-1111

Referencia: ID-104223

ANEXO 1

Tabla 1

**Productos de Auditoría respecto a:
Ciberseguridad, planes de continuidad tic, estrategias de recuperación, continuidad del negocio, gestión de crisis, medidas de contingencia, EDUS y EDAC**

N° de oficio y fecha	Asunto	Aspectos comunicados a la administración activa
<p>ATIC-213-2017 del 19 de diciembre de 2017</p>	<p>Evaluación de carácter especial referente al avance del proyecto EDUS en cumplimiento de lo establecido en la Ley no. 9162</p>	<p><i>“(...) Los resultados del informe evidenciaron oportunidades de mejora relacionadas con el avance en la puesta en marcha de las aplicaciones del Expediente Digital en los establecimientos de salud de los diferentes niveles de atención definidos en la Institución, lo cual, de no implementarse medidas pertinentes en forma inmediata, podría generar que no se cumpla con los plazos establecidos en el transitorio único de la Ley Expediente Digital No.9162.</i></p> <p><i>En ese sentido, es relevante mencionar que no se aprecia una visión integral del proyecto EDUS, que responda a los alcances y objetivos fijados en la norma citada supra, comprometiendo no solo la atención de los asegurados, sino la imagen de la Institución (...)</i></p> <p><i>Finalmente, se comprobó la ausencia en la definición de una solución integral de contingencia a las aplicaciones EDUS ARCA, lo cual es vital para garantizar disponibilidad de la información institucional en salud ante eventos que afecten la continuidad de los servicios automatizados.</i></p>
<p>ATIC-244-2018 del 21 de diciembre de 2018</p>	<p>Auditoria de carácter especial referente a la implementación del Expediente Digital Único en Salud (EDUS) y uso de las soluciones tecnológicas que lo conforman.</p>	<p><i>“(...) Al respecto, se determinaron los siguientes aspectos de mejora, relacionados con la continuidad de los servicios de salud entre los cuales se pueden mencionar:</i></p> <ul style="list-style-type: none"> <i>• Que el EDAC disponga de la funcionalidad de registro de datos, ya que solo permite la consulta de pacientes atendidos durante la interrupción.</i> <i>• Adicionalmente, es necesario que dicho software contemple los procesos que se automatizan a través de los sistemas ARCA tales como: Admisión y Egresos, Módulo Quirúrgico y Patología</i> <i>• Disponer de un mecanismo o lineamiento oficializado para que las atenciones médicas realizadas durante los procesos de interrupción sean incluidas posteriormente en el EDUS-ARCA.</i> <i>• En visitas efectuadas a los establecimientos adscritos de las cinco direcciones regiones de la red de servicios de salud, se evidenció que el principal mecanismo para la continuidad de los servicios de salud es el uso del expediente físico (...)</i>”.
<p>AS-ATIC-2563-2021 del 6 de diciembre de 2021</p>	<p>Oficio de asesoría referente al informe sobre resultados de la implementación del EDUS y propuesta de conservación y/o</p>	<p><i>“(...) Es preciso considerar que el funcionamiento del Expediente Digital Único en Salud es una solución tecnológica, cuya ley que lo regula, estableció características técnicas como lo son, seguridad, escalabilidad, usabilidad, portabilidad, integridad, trazabilidad, entre otros. Asimismo, señala que debe</i></p>



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

	<p>transformación de la estructura funcional actual.</p>	<p><i>atender los objetivos funcionales y las funcionalidades que requieren los servicios de salud en los tres niveles de atención, incluyendo soluciones informáticas para la implementación de la receta electrónica, la gestión telemática de citas y la imagenología digital, sistema de interconsulta y referencia y contrarreferencia (...)</i></p> <p><i>Tal y como se ha indicado, es necesario efectuar una revisión general de cada una de las estructuras organizacionales creadas desde el 2015 y mantenidas a través del tiempo en el contexto del proyecto EDUS, siendo que el mismo fue dado como cumplido en setiembre del 2018, para que se revisen roles y responsabilidades ya establecidas en los manuales de organización de las unidades programáticas involucradas. Esa valoración debe efectuarse, bajo una visión de rendición de cuentas y aprovechamiento de los recursos institucionales (...)</i></p>
<p>AD-ATIC-706-2020 del 16 de marzo de 2020</p>	<p>Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre del 2019.</p>	<p><i>"(...) según lo esbozado en el presente oficio, se identificaron debilidades en la gestión de la continuidad que evitaron el ofrecer a los usuarios la seguridad de mantener en operación los procesos asociados a servicios de telefonía, cómputo, internet y sistemas de información, esto sin disponer de elementos de contingencia que permitieran abordar el evento en el menor tiempo posible y con el mínimo impacto.</i></p> <p><i>No obstante, la Caja Costarricense del Seguro Social, demanda la alta disponibilidad de los servicios tecnológicos que apoyan los procesos de salud, pensiones y recaudación patronal, lo cual hace considerar la interrupción acontecida en el pasado octubre 2019, siendo necesario analizar estratégicamente lo evidenciado en aras de establecer las medidas que garanticen la continuidad razonable de los procesos y así evitar la futura exposición a vulnerabilidades de seguridad, esto contextualizado en las disponibilidad de planes de contingencia para el negocio y de las tecnologías de información y comunicaciones.</i></p> <p><i>Al respecto la integralidad para la gestión de la continuidad de negocio y las tecnologías de información y comunicaciones deberán minimizar riesgos, por cuanto esto genera una asociación entre todos los esfuerzos que se llevan a cabo en la institución, orientados a velar por la prevención, protección y recuperación ante eventos de interrupción o desastre (...)</i></p> <p><i>Asimismo, se ha de considerar el generar acciones posteriores a las incidencias para incentivar la generación del aprendizaje necesario, en aras de retroalimentar los planes de continuidad en las unidades programáticas de la Institución, así como otras iniciativas y esfuerzos relacionadas al tema (...)</i></p>



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

<p>AS-AATIC-072-2022 del 10 de junio de 2022</p>	<p>Oficio de Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.</p>	<p><i>“(…) En virtud de lo anterior y bajo el contexto actual de la CCSS, es menester de este Órgano Fiscalizador hacer recordatorio a la Administración sobre la importancia que reviste al tema de gestionar la crisis ante los ciberataques, principalmente considerando el impacto y la exposición prolongada a la desconexión de los sistemas de información en la institución. (…)</i></p>
<p>AS-AATIC-088-2022 del 16 de junio de 2022</p>	<p>Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico.</p>	<p><i>“(…) La Caja Costarricense del Seguro Social (CCSS), dentro de su gestión y servicios que presta a la ciudadanía depende de la información, sistemas y soluciones tecnológicas, entre otros procesos; de ahí la necesidad de disponer de un sistema de gestión para la continuidad del negocio.</i></p> <p><i>Lo anterior, en aras de que la Institución en cada uno de los procesos de salud, pensiones y recaudación patronal disponga de herramientas o soluciones capaces de aportar valor cuando las actividades sustantivas permanezcan ininterrumpidas, por fallas de origen eléctrico, financiero, tecnológico, eventos de seguridad, desastres naturales, entre otros.</i></p> <p><i>(…) se previene a esa Administración sobre lo indispensable que resulta la adopción de un plan de continuidad del negocio, debidamente integrado y con mecanismos de contingencia oportunos; basado la estandarización de soluciones, identificación de valores críticos, aplicación de normas y metodologías oficializadas en la institución; así como valorando lo indicado en marcos referenciales de buenas prácticas que permitirían construirlo, ponerlo en marcha o perfeccionarlo (…)</i>”.</p>
<p>AS-AATIC-108-2022 del 22 de junio de 2022</p>	<p>Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico.</p>	<p><i>“(…) se pretende que, a partir de las observaciones inmersas en esta misiva, se valore la definición de la estrategia más apropiada a los requerimientos específicos de la Caja, su apetito al riesgo y de la disponibilidad de recursos.</i></p> <p><i>(…) involucrando a los sistemas de información, aplicativos, datos, equipamientos tecnológicos y otros elementos vitales en cualquier plan de continuidad del negocio, así como los contingenciales de los servicios de apoyo, entre ellos los correspondientes a las TIC.</i></p> <p><i>Así mismo, destacando la necesidad inminente de fortalecer las soluciones de alta disponibilidad y la generación de acciones preventivas que prevengan y minimicen la posibilidad de ocurrencia ante desastres a nivel nacional.</i></p> <p><i>Todo lo anterior, con el objetivo de ser resilientes y generar confianza en los servicios que obtienen apoyo por parte de las TIC, manteniendo la continuidad de las operaciones, pese al costo en inversión necesaria para prever este tipo de eventos (mínimo, en comparación a una nueva materialización del riesgo), de ahí la relevancia de la</i></p>



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

		<p>temática de valoración y priorización detallada en este oficio (...)."</p>
<p>AS-AATIC-113-2022 del 27 de junio de 2022</p>	<p>Oficio de Asesoría sobre el restablecimiento en la operación de sistemas de información y bases de datos.</p>	<p>"(...) esta misiva incluye observaciones para incentivar la implementación de valoraciones de alta calidad, reforzar el entorno TIC buscando y cerrando brechas.</p> <p>Es decir, complementando esa premisa con la seguridad de haber mitigado los riesgos materializados en los dispositivos y/o redes informáticas, al instalar las actualizaciones correspondientes y soluciones de protección especializadas, necesarias de forma preliminar para determinar si es el momento de proceder con el restablecimiento de servicios tecnológicos en un ambiente controlado.</p> <p>Finalmente, habiendo examinado los aspectos de ciberseguridad citados, se debe proceder a la valoración por parte de cada estructura organizacional, la directriz a seguir para la migración de información generada en los mecanismos contingenciales (durante la interrupción de servicios tecnológicos) a las bases de datos vinculadas a sus respectivos sistemas de información estandarizados para apoyar los procesos sustantivos de la Institución (...)."</p>
<p>AS-AATIC-116-2022 del 07 de julio de 2022</p>	<p>Oficio de Asesoría referente a los Planes de Continuidad de TIC.</p>	<p>"(...) Los Planes de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, deben tener como objetivo garantizar la recuperación de los equipos y sistemas críticos posterior a la materialización de un riesgo, además de establecer políticas y procedimientos que reduzcan en la medida de lo posible la afectación o suspensión de los servicios que se brindan a los usuarios.</p> <p>(...) resulta necesario que, los diferentes actores involucrados: Dirección de Tecnologías de Información y Comunicaciones, Área de Seguridad y Calidad Informática, Subárea de Continuidad de la Gestión, Centros de Gestión Informática gerenciales, regionales y locales, entre otros; efectúen una revisión y análisis de la calidad y eficacia de la estrategia actual establecida en torno a los Planes de Continuidad de la Gestión de TIC (contingencias requeridas y capacidad de replicación), su alcance (establecimiento de riesgos y vulnerabilidades), actualización (con el objeto de reflejar siempre la realidad del entorno), políticas y procedimientos con referencia a la continuidad de las operaciones (para identificar las principales regulaciones nacionales e internacionales de aplicación en la materia), así como, de los procesos de respaldo de los sistemas informáticos y bases de datos, de modo que se garantice el cumplimiento de los objetivos institucionales establecidos y la continuidad de los procesos de salud, pensiones y recaudación patronal, según corresponda (...)."</p>
<p>AS-AATIC-135-2022 del 11 de julio de 2022</p>	<p>Oficio de Asesoría sobre el impacto en la prestación de servicios y medidas de contingencia,</p>	<p>"(...) Con el paso del tiempo, los ciberdelincuentes se vuelven más sofisticados, organizados, persistentes y económicamente motivados, por lo que, para protegerse y recuperarse de un ciberataque, la organización debe</p>



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincecs@ccss.sa.cr

	<p>producto del ataque cibernético en la plataforma tecnológica institucional.</p>	<p><i>implementar un plan eficaz de respuesta, una plataforma que reúna defensas inteligentes, robustas, resilientes y organizadas, así como, la definición de roles específicos, responsabilidades claras y medios de comunicación previamente definidos (para evitar ambigüedad y confusión en la información).</i></p> <p><i>La comunicación con los funcionarios y usuarios de los servicios (médico, administrativos y financieros) debe ser constante tras un ciberataque, ya que se debe conocer el alcance del incidente y las medidas de respuesta y contingencia establecidas por las autoridades institucionales; asimismo, es importante abordar una estrategia de monitorización de redes sociales para analizar cómo está afectando el ciberataque a los usuarios y a la imagen institucional, y así poder dar una respuesta oportuna y transparente, para generar confianza.</i></p> <p><i>(...) En relación con lo anterior, esta Auditoría considera necesario establecer una estrategia integral en conjunto con todos los niveles organizacionales, con el fin de efectuar una revisión y análisis de las actuaciones previas y posteriores al ataque cibernético en la plataforma tecnológica institucional a partir del 31 de mayo del 2022, así como sus efectos en la continuidad del negocio, con el propósito de documentar lecciones aprendidas (en los niveles centrales, regionales y locales), en torno a evitar una situación similar en el futuro y/o mejorar la capacidad de reacción institucional ante eventos de este tipo o cualquiera que atente contra la prestación de servicios (...).</i></p>
<p>AS-AATIC-147-2022 19 de julio de 2022</p>	<p>Oficio de Asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social.</p>	<p><i>“(...) se considera relevante la participación y empoderamiento del Consejo Tecnológico, en la premisa de generar de valor agregado para asegurar la gobernanza y gestión de las TIC y de la seguridad de la información, donde se incluyen cierre brechas e iniciativas asociadas con el ejercicio de roles y responsabilidades en seguridad de la información y ciberseguridad. En otras palabras, la alta dirección debe tomar conciencia y liderazgo en priorizar y dar seguimiento a los proyectos que pretenden aumentar las capacidades a la CCSS.</i></p> <p><i>Así las cosas, ese accionar busca asegurar que los roles, responsabilidades y autoridades sean claros para el sistema de gestión de seguridad y a partir de ello, las partes interesadas (entre ellas la DTIC y unidades a cargo) desplieguen lo correspondiente a nivel estratégico, táctico y operativo para adaptarse a las necesidades del negocio, bajo el ordenamiento de prioridades y la articulación de esfuerzos (...)</i></p> <p><i>Además, reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI, al construir una estructura con roles y responsabilidades acorde a las</i></p>



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: coincss@ccss.sa.cr

<p>AS-AATIC-147-2022 19 de julio de 2022</p>	<p>Oficio de Asesoría referente a mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas.</p>	<p><i>perspectivas de ciberseguridad y/o disposición de: normas actualizadas (...)</i></p> <p><i>"(...) Tal y como se indicó supra, es necesario disponer de un plan que propicie de manera razonable la continuidad de los servicios, incluyendo la generación de respaldos de archivos de imágenes médicas, garantizando la eventual recuperación en caso de falla o pérdida, considerando dentro de esa planificación los sitios donde se almacenarían y la periodicidad con que deben efectuar. Lo anterior, debido a la importancia de estos medios para la elaboración de diagnóstico y tratamiento en beneficio de los pacientes.</i></p> <p><i>Si bien es cierto, le corresponde a cada establecimiento de salud establecer e implementar los mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas, continúa siendo prioridad la estrategia de implementación de la solución institucional Red Digital Institucional de Imágenes Médicas (REDIMED).</i></p> <p><i>(...) se hace necesario establecer y documentar los procedimientos de pruebas y protocolos necesarios para asegurar la operación y funcionamiento del sistema de imágenes en caso de presentar falla, siendo que la institución debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios (...)</i></p>
<p>ATIC-129-2022 del 19 de diciembre de 2022</p>	<p>Auditoría de carácter especial sobre el uso e implementación integral de los sistemas de información que conforman el Expediente Digital Único en Salud (EDUS), así como otros componentes asociados requeridos para su funcionamiento a nivel institucional.</p>	<p><i>"(...) En virtud de lo expuesto, este Órgano de Fiscalización institucional ha solicitado la conformación de un equipo interdisciplinario responsable de efectuar un diagnóstico actual de la gobernanza del EDUS mediante la implementación de roles del Comité Ejecutivo EDUS, Comité Gestor EDUS, entre otros equipos de trabajo que intervienen en la toma de decisiones y gestión de análisis, desarrollo e implementación en torno al EDUS (...)</i></p> <p><i>Además, con la asesoría de la Dirección de Tecnologías de Información y Comunicaciones, elabore un plan de trabajo con plazos, responsables y actividades orientadas a la valoración de alternativas de solución al corto, mediano y largo plazo para disponer de una solución tecnológica contingente que permita la continuidad de servicios ante una eventual interrupción o falla del EDUS y establecer un proceso de gestión de la calidad de información administrada mediante el EDUS a través del cual se realicen revisiones periódicas basadas en protocolos y/o metodologías debidamente reguladas en materia de protección de datos y ciberseguridad que garantice razonablemente la integridad de la información (...)</i></p>

Fuente: Elaboración propia de Auditoría.