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

Al contestar refiérase a: **ID-120071**

AD-ATIC-0080-2024
19 de julio de 2024

Doctor
Alexander Sánchez Cabo, gerente a.i
GERENCIA MÉDICA – 2901

Máster
Leslie Vargas Vásquez, jefe a.i.
Área Estadísticas en Salud
GERENCIA MÉDICA – 2901

Estimado(a) señor(a):

ASUNTO:	**Oficio de Advertencia sobre los mecanismos de control establecidos respecto al acceso a la información consignada en el Expediente Digital Único en Salud de la Caja Costarricense del Seguro Social, perteneciente a los usuarios o titulares de los datos en concordancia con la *Ley No. 8968*[1].**

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2024 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, emite la siguiente advertencia sobre la justificación de acceso al Expediente Digital Único en Salud (EDUS) de la Caja Costarricense del Seguro Social (CCSS) por parte de los perfiles de Expediente General y Consultor Expediente, entre otros de similar naturaleza, detallando los siguientes aspectos a valorar para la toma de decisiones y acciones que compete a esa Administración.

I- GENERALIDADES

El Expediente Digital Único en Salud es un sistema electrónico que integra la información médica de los pacientes en un solo lugar accesible por los profesionales de la salud autorizados. Este sistema permite el acceso a la información clínica de los pacientes, facilitando la atención médica, la toma de decisiones, la interoperabilidad de los datos y la coordinación entre diferentes instituciones de salud.

Para tales efectos, la implementación del Expediente Digital de Salud fue declarado de interés público, a través de la Ley de Expediente Digital Único en Salud (EDUS) No. 9162, del 23 de setiembre de 2013, en la cual se menciona la finalidad de este, a saber:

> *"(…) establecer el ámbito y los mecanismos de acción necesarios para el desarrollo del proceso de planeamiento, financiamiento, provisión de insumos y recursos e implementación del expediente digital único de salud, desde una perspectiva país.*
>
> *Para dicho fin, se entiende por expediente digital único de salud el repositorio de los datos del paciente en formato digital, que se almacenan e intercambian de manera segura y puede ser accedido por múltiples usuarios autorizados. Contiene información retrospectiva, concurrente y prospectiva, y su principal propósito es soportar de manera continua, eficiente, con calidad e integralidad la atención de cuidados de salud."*

[1] Ley No. 8968 referente a la Protección de la Persona frente al tratamiento de sus datos personales.

Dado lo anterior, la plataforma digital EDUS, se implementó desde el 2018 en la Institución, y constituye un conjunto de aplicativos integrados y asociados a un repositorio de datos, el cual es accedido por los usuarios debidamente autorizados, bajo las consideraciones de la propiedad del EDUS, según lo establece el Reglamento de la Ley No.9162, señalando:

> *"El expediente digital único de salud en su concepto, diseño, operación, plataforma tecnológica, códigos fuentes, soluciones de valor orientados al titular de los datos y demás contenido material del EDUS son propiedad exclusiva de la CAJA.* ***La información derivada de la atención de los usuarios de los servicios de salud o del titular de los datos, con las limitaciones que establece el artículo 9 inciso d) de la Ley No. 8968, pertenece a estos usuarios o titulares de los datos****" (El resaltado no es parte del original).*

Ahora bien, dada la naturaleza de la información que se almacena en la base de datos, la implementación de mecanismos de seguridad física y lógica, para la protección de los registros, los aplicativos y sistemas, contra accesos no autorizados o la continuidad de los servicios asociados, es de suma importancia en aras de evitar inconvenientes en la gestión institucional.

En ese sentido, el EDUS debe alinearse al cumplimiento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales No. 8968, normativa interna de la CCSS y otras consideraciones orientadas a que la solución tecnológica contenga medidas básicas de seguridad, con el objetivo de garantizar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad del componente tecnológico de marras.

Usuarios con acceso a los datos contenidos en el EDUS

En concordancia con lo anterior, existen múltiples usuarios en el EDUS[2] que pueden o deben acceder al repositorio de información para desempeñar sus labores. En todos los casos, dichos funcionarios están obligados a tratar adecuadamente los datos personales y a resguardar el secreto profesional o funcional.

A manera de ejemplo, los perfiles de Consultor Expediente General y Consultor Expediente, entre otros de similar naturaleza deben registrar el motivo que justifica el acceso al expediente de una persona en modo de lectura, sin posibilidad de realizar modificaciones, en aras de resguardar la privacidad de la información consultada y abstenerse de acceder sin una razón adecuada (acceso no autorizado). En caso contrario, se enfrentarán a las consecuencias disciplinarias y administrativas; además de las consecuencias civiles y penales que el ordenamiento jurídico impone.

2. OBSERVACIONES

El Sistema EDUS facilita el acceso a los expedientes médicos para los funcionarios que lo requieren en función del servicio que prestan a la Institución. Para estos efectos, los usuarios del sistema de información deben cumplir con los deberes y responsabilidades relacionados con el tratamiento de los datos personales de cada individuo identificado en la(s) base(s) de datos de la CCSS, con un fiel apego al principio de confidencialidad. Lo anterior tiene como objetivo garantizar que la información permanezca accesible solo para quienes tienen el derecho y la necesidad legítima de conocerla.

[2] Usuario del EDUS: Persona física legitimada debido a su función, nombramiento o relación con la CAJA, (se incluye todos aquellos profesionales en salud en calidad de docentes, así como terceros autorizada por convenio, contrato u otra forma de relación jurídica), que esté expresamente autorizada conforme con este Reglamento y regulaciones específicas, para acceder a los datos contenidos en el EDUS e incluir nuevos datos o registros, actualizar, modificar o consultar; según corresponda su función y nivel de acceso asignado al usuario autorizado. Todo usuario del EDUS se encuentra sujeto al deber de confidencialidad.12

A ese respecto, en el oficio AD-AATIC-103-2022, esta Auditoría Interna enfatizó la necesidad de implementar alertas para detectar accesos irregulares a la información. Estas alertas deben anticipar situaciones que se desvíen de patrones predeterminados, acciones sospechosas o justificaciones improcedentes.

Además, se subrayó la importancia de supervisar la calidad de las justificaciones utilizadas para acceder a la información del EDUS.

Ahora bien, la respuesta dada en oficio GM-AES-1-0018-2023 09 de enero de 2023 a dicho pronunciamiento fue:

> *"**Observación N°1: Sobre la generación de alertas en el acceso de la información sensible y automatización de estado de suspensión e inhabilitación de usuarios MISE***
>
> *-Se realiza sesión de trabajo el día 06 de diciembre de 2022 con representación de los gestores EDUS regionales de la Central Norte y Central Sur, para identificar mecanismos de alertas en el acceso de información del EDUS con base a la propuesta realizada por el equipo.*
>
> ***Observación N°2 Supervisión de calidad aplicada a las justificaciones dadas para acceder a información sensible del EDUS***
>
> *-Mediante oficio GM-14102-2022GG-DTIC-6755-2022 con asunto "Informe de avance sobre el cumplimiento de la disposición de Contraloría General dela República 4.5 del Informe de Auditoría de Carácter Especial sobre la Seguridad de la Información del Expediente Digital Único en Salud (EDUS) en la Caja Costarricense de Seguro Social N° DFOE-BIS-IF-00002-2022" se procede con revisión de la asignación de roles y perfiles de los aplicativos del EDUS asignadas a los funcionarios con categoría de puesto no son correspondiente con perfiles de atención directa de pacientes y en los de usuarios jubilados, fallecidos.*
>
> *-Aunado a lo anterior, en oficio GM-14287-2022 con fecha 28 de noviembre de 2022 con "Asunto: Deshabilitación de perfiles inactivos en aplicativos EDUS en cuentas con fecha de caducidad mayor a 120 Días" y se comunica a los directores de Sede, Direcciones de Redes Integradas, Prestación de Servicios de Salud, Direcciones Generales de Hospitales Nacionales y Especializados, Direcciones Generales de Hospitales Regionales y Periféricos y Direcciones Médicas de Área de Salud de la CCSS."*

Así mismo, en oficio GM-AES-1-0039-2023 del 12 de enero del 2023, el Área de Estadísticas en Salud indica que se ha elaborado una hoja de ruta para definir acciones de planificación, implementación, control y seguimiento de los mecanismos de seguridad concernientes a la confidencialidad en el tratamiento de los datos personales, por parte de los usuarios del EDUS, conforme a las observaciones del oficio de advertencia de la Auditoría interna.

En ese sentido, el plan en cuestión detalla las acciones previstas para abordar los temas identificados por esta Auditoría. En cuanto a las actividades, se establecía como meta principal alcanzarlas a más tardar en diciembre de 2023.

Por otra parte, el producto emitido por este Órgano Fiscalizador AS-ATIC-0021-2024 insistía en la necesidad de retomar dichos temas, previamente mencionados en el oficio de advertencia AD-AATIC-103-2022. En respuesta a dicho pronunciamiento en oficio GM-5895-2024 / GM-AES-1-0690-2024 del 22 de abril de 2024, cita:

> *"Mediante oficios GM-AES-1-0018-2023 y GM-1-AES-0039-2023, el M.Sc. Leslie Vargas Vásquez, jefe a.i del Área de Estadística en Salud, traslada al Dr. Randall Álvarez Juárez, Gerente Médico (anterior) y Msc. Olger Sánchez Carrillo, Auditor, las acciones realizadas en atención a la nota GM-13175-2022, relacionado con oficio AD-AATIC-103-2022 de Advertencia referente al fortalecimiento de los mecanismos de control asociados con la premisa de garantizar la confidencialidad de la información contenida en el Expediente Digital Único en Salud (EDUS) de la Caja Costarricense del Seguro Social (CCSS), respectivamente.*

En el mismo se traslada y adjunta la hoja de ruta referente al fortalecimiento de los mecanismos de control asociados con la premisa de garantizar la confidencialidad de la información contenida en el Expediente Digital Único en Salud (EDUS).

También, mediante oficios GM-AES-1-0694-2024, se traslada segundo informe sobre las acciones realizadas en la hoja de ruta definida, al Dr. Doctor Wilburg Diaz Cruz, Gerente Médico, y Máster Olger Sánchez Carrillo, Auditor Interno, como parte del seguimiento a las acciones de planificación, implementación, control y seguimiento de los mecanismos de seguridad concernientes a la confidencialidad en el tratamiento de los datos personales, conforme a las observaciones del oficio de advertencia de la Auditoría interna.

De lo anterior, demuestra que para esta Gerencia los temas control asociados en garantizar la confidencialidad de la información contenida en el EDUS son relevantes, por lo cual se le brinda el seguimiento respectivo, con el fin de fortalecer los procedimientos establecidos."

En ese contexto, el oficio *GM-AES-1-0694-2024 del 25 de abril del 2024* especifica que las acciones orientadas a la generación de alertas están completas y en relación con el objetivo de supervisar la calidad de las justificaciones, cita:

"De las 4 actividades definidas solamente se encuentra pendiente de completar la correspondiente a "Implementar evaluaciones de cumplimiento que señale planes de mejora", la cual se encuentra en estado de iniciado, con relación en el informe se anexa los oficios de evidencia de las acciones realizadas."

No obstante, es crucial destacar la importancia de este tema debido a los riesgos que enfrenta la Institución al manejar información sensible, como la posibilidad de un manejo inadecuado por parte de funcionarios que, en ciertas situaciones, pueden aprovechar los privilegios asignados para fines distintos a los conferidos por la CCSS o no cumplir adecuadamente con los deberes relacionados con el manejo de datos personales.

Esto se menciona porque la Auditoría ha tenido conocimiento de casos en los cuales usuarios de los servicios prestados por la CCSS han presentado denuncias indicando accesos indebidos a sus expedientes médicos. En algunos de estos, se ha procedido a iniciar procedimientos administrativos e incluso denuncias penales que, además de establecer el orden y respetar la normativa, su incumplimiento generan daños reputacionales y económicos a la Institución.

Bajo ese contexto, la CCSS no debería conformarse con las medidas de control actuales, ni asumir que no pueden afinarse; es fundamental identificar continuamente oportunidades de mejora para evitar la vulneración de la confidencialidad de los datos de identificación, historias clínicas y otra información relacionada con la salud de los pacientes.

En este contexto, y con el propósito de ilustrar la situación, este Órgano Fiscalizador realizó un análisis de los registros de acceso a expedientes médicos digitales en el EDUS por parte de funcionarios con el perfil de usuario "Consultor de expediente general" durante el mes de febrero de 2024. Este perfil registró 479,767 consultas realizadas por 9,801 consultores de expediente general.

A partir de lo observado, se identificaron aleatoriamente los siguientes casos que alertan sobre la justificación proporcionada por los profesionales para acceder a los datos contenidos en el EDUS, a saber:

Tabla No. 1
Justificación de acceso al consultar expedientes médicos
Perfil: Consultor de expediente general, febrero 2024

No de consultas	Justificación del profesional médico que motivó la consulta	Funcionario
68	Patrones de texto similares a: • 00000000000000000000000000	EFRAIN RAMIREZ FONSECA 2104 - HOSPITAL MEXICO
46	Patrones de texto similares a: • SSSSSSSSSSSSSSS • XXXXXXXXXXXXXXXX • ZZZZZZZZZZZZZZZZZZZZZZZZZZZZ	ABDY OROZCO MONTOYA 2314 - AREA DE SALUD ZAPOTE-CATEDRAL
40	• REVISION EXPEDIENTE	ADELINA CHINCHILLA PANIAGUA 233306 - EBAIS DULCE NOMBRE
132	Patrones de texto similares a: • AAAAAAAAAAAAAAAAAAAAAAAAAAAA • BBBBBBBBBBBBBBBBBBBBBBBBBB • BGGGGGGGGGVVVVVVVVVVVV • CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC • DDDDDDDDDDDDDDDDDDDDDDDDDDDDD • FFFFFFFFFFFFFFFFFFFFFFFF • GGGGGGGGGGGGGGGGGGGGGGGGG • JJJJJJJJJJJJJJJJJJJJJJJJJJ • KKKKKKKKKKKKKKKKKKKKKK • NNNNNNNNNNNNNNNNNNNNNNNNN • RRRRRRRRRRRRRRRRRRRRRRRRRR • SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS	ADILIA DAMARIS DIAZ MENDOZA 2314 - AREA DE SALUD ZAPOTE-CATEDRAL
51	CONSULTA DE EXPEDIENTE	ADRIAN GUZMAN RAMIREZ 2306 - HOSPITAL MAXIMILIANO PERALTA JIMENEZ
35	VALORACION DE EXPEDIENTE	ADRIAN JOSE SOLORZANO SUAREZ 2347 - AREA DE SALUD SAN SEBASTIAN-PASO ANCHO
155	Patrones de texto similares a: • REVIOSION DE EXP • REVISAR EL EXP • REVISIO DE EXZP • REVISIOJN DE EXP • REVISION DE EXP	GABRIELA BARRANTES MIRANDA 2217 - AREA DE SALUD CORONADO
209	Patrones de texto similares a: • XCONSULTA EXPEDIENTE • CONSULTAR EXPEDIENTE • CONSULTA EXPEDIENTE • CONSULTA DE EXPEDIENTE • COMSULTA EXPEDINTDE • CONSULRA EXPEDIENTE	ENRIQUE SANCHEZ VUELVAS 2104 - HOSPITAL MEXICO
22	Patrones de texto similares a:	PRISCILLA MARIA OVARES GRANADOS

No de consultas	Justificación del profesional médico que motivó la consulta	Funcionario
	• AHCAJSBCBSAZCLJSABCB JSHCKAS • AKSFCASJHBHCFKASJLKJCKSABJFCB • ASJCHASJHCASKCOASWCUDASHGCH • AWDCFAWSGFCHAJKCOAWJC • EWHFCESAGHFCSAKFCKHSAJGFCJHVDSHVC • HGHGVHGVHKJLKJLKJLKMLKMNKJN	2801 - CENTRO NACIONAL DE CONTROL DEL DOLOR Y CUIDADOS PALIATIVOS

Fuente: A partir de la información suministrada en el oficio GM-AES-4-1030-2024 del 24 de junio del 2024 suscrito por el Lic. Michael Rodriguez Cordero Jefe a.i del Área de Estadística en Salud.

A ese respecto, los ejemplos evidencian patrones de texto irregulares en las justificaciones dadas por los funcionarios para acceder a los expedientes médicos en el sistema EDUS, práctica que podría señalar debilidades en la forma de documentar las actividades efectuadas por los profesionales o intentos de ocultar o falsificar la verdadera razón para acceder a la información; en cualquier caso, son motivos de preocupación en términos de la autodeterminación, seguridad y confidencialidad de los datos.

Sin embargo, cabe destacar que lo analizado por la Auditoría es un extracto de muchos casos que podrían presentar esta situación; evidenciándose la ausencia de mecanismos de alerta o control ajustados a las necesidades de la Caja y, consecuentemente, aspectos de supervisión que no están siendo efectuados para mitigar la exposición al riesgo.

En este contexto, se advierte sobre el escenario citado y la necesidad urgente de implementar acciones que permitan fortalecer las áreas correspondientes.

II- CONSIDERACIONES NORMATIVAS

En relación con los temas antes indicados existe un conjunto de leyes, normas, reglamentos y demás documentos que señalan deberes, derechos, definiciones y objetivos vinculados con la premisa de garantizar la confidencialidad y/o privacidad de la información, a saber:

Según lo establecido en la Ley No. 8239 Deberes y Derechos de las Personas Usuarias de los Servicios de Salud Públicos y Privados, los usuarios de los servicios de salud tienen derecho a recibir atención médica con la eficiencia y diligencia debida, bajo criterios de confidencialidad, tal y como se señala en el artículo 2, inciso m:

> *"**ARTÍCULO 2.- Derechos***
> *Las personas usuarias de los servicios de salud tienen derecho a lo siguiente:*
> *"m) Hacer que se respete el **carácter confidencial de su historia clínica y de toda la información relativa a su enfermedad** salvo cuando, por ley especial, deba darse noticia a las autoridades sanitarias. En casos de docencia, las personas usuarias de los servicios de salud deberán otorgar su consentimiento para que su padecimiento sea analizado." **El resaltado no es parte del original.***

La ley No. 8968 "Protección de la Persona frente al tratamiento de sus datos personales", define en el Artículo 3 "Definiciones", los tipos de datos y el deber de confidencialidad, citando:

> *"**b)** Datos personales: cualquier dato relativo a una persona física identificada o identificable.*
> ***c)** Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.*
> ***d)** Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.*

> ***e)*** *Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.*
> ***f)*** *Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos"*

Esa misma Ley de Protección de la Persona frente al tratamiento de sus datos personales, establece en su Artículo 11 "Deber de confidencialidad", lo siguiente:

> *"La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce."*

En ese sentido, la Ley No. 9162 del EDUS, en el artículo 11, establece la clasificación y tratamiento de los datos contenidos en expediente en salud, a saber:

> *"Toda información contenida en el expediente digital único de salud se considera* ***información privada que contiene datos sensibles****. Se prohíbe el tratamiento de dichos datos y el responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para* ***garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado****.*
>
> *Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual para garantizar la protección de la información almacenada.*
>
> ***El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional o funcional****, aun después de finalizada su relación con la base de datos". **El resaltado no es parte del original.***

El reglamento a dicha Ley determina en el artículo 1, las definiciones de la confidencialidad de los datos contenidos en el EDUS, asociado con los deberes y obligaciones a nivel CCSS que refieren al tema, citando:

> *"**Confidencialidad**: Condición inherente a los datos contenidos en el EDUS correspondientes a una persona física identificada o identificable, cuya divulgación no autorizada constituye un delito penado con multa, prisión y/o inhabilitación para el ejercicio de cargos públicos, de conformidad con el artículo 203 y 196 bis del Código Penal.*
>
> *(…)* ***Deber de confidencialidad****: Obligación de todos los usuarios del EDUS con acceso a los datos, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la Ley del Expediente Digital Único de Salud (EDUS) No 9162 y el secreto profesional, principalmente cuando se acceda a información sobre datos personales, restrictos y sensibles.*
>
> *Esta obligación perdurará aun después de finalizada la relación con el sistema de información, con la Institución o haya terminado su relación laboral por terceros".*

Además, en el Artículo 8 "Área de Estadística en Salud", se detalla la función de áreas técnicas que velan porque el acceso al expediente de salud, físico o digital cumpla con los lineamientos de confidencialidad, a saber:

> *"Es la dependencia técnica institucional, encargada de la normación y regulación técnica del EDUS, para lo cual estará facultada para realizar las coordinaciones necesarias, con las instancias técnicas pertinentes, para la integración de los distintos módulos relacionados con el proceso de atención, la generación de productos de información en salud, con estricto apego a este reglamento y normativa conexa, incluyendo las regulaciones sobre trámite, custodia, uso, conservación de los expedientes y bases de datos en salud, digitales y físicos, de acuerdo con la realidad institucional y tecnológica, en orientación a la estandarización e igualdad de los procesos de atención en los distintos niveles de la red de servicios.* ***En cualquier caso, el AES debe velar porque el acceso al expediente de salud, físico o digital cumpla con los lineamientos de confidencialidad****". El resaltado no es parte del original.*

En ese mismo cuerpo normativo, en el Artículo No. 19 "Confidencialidad y secreto profesional" puntualiza la criticidad de los datos contenidos en los aplicativos del EDUS, citando:

> *"**La información, datos y en general registros contenidos en los aplicativos del EDUS son confidenciales**. La obligación de observar esta disposición general incluye a los usuarios de EDUS que por motivo de su labor tengan acceso a dicha información, por lo que **su violación acarreará las consecuencias disciplinarias y administrativas** que correspondan, sin menoscabo de las consecuencias civiles y penales que el ordenamiento jurídico impone. En protección de la confidencialidad, los usuarios autorizados para acceder al contenido de las bases de datos del EDUS se acreditarán conforme al nivel de acceso asignado que corresponda, según el uso estrictamente necesario para el adecuado cumplimiento de su función, en concordancia con lo dispuesto en el presente reglamento. El deber de confidencialidad se mantiene aún después de finalizada la relación con el EDUS. El secreto profesional se rige por lo establecido en el artículo 203 del Código Penal." **El resaltado no es parte del original.***

Las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), en el inciso 5.7. "Calidad de la comunicación", señala lo siguiente:

> *"**5.7.4 Seguridad***
> *Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."*

III- PRODUCTOS DE FISCALIZACIÓN RELACIONADOS AL TEMA

Sobre el particular, esté Órgano Fiscalizador ha emitido cuatro productos que refieren concretamente a temas relacionados con el tratamiento de sus datos personales, a saber:

Tabla No. 1
Productos emitidos por la Auditoría en Tecnologías de Información y Comunicaciones sobre la Protección de Datos Personales y Salud

Informe	Fecha	Asunto
ATIC-83-2018	27 de julio del 2018	Evaluación de carácter especial referente al cumplimiento de la Ley No. 8968 Protección de la Persona frente al tratamiento de sus datos personales en la CCSS.
ATIC-41-2021	24 de mayo del 2021	Evaluación de carácter especial referente a la gestión técnica y administrativa de la aplicación móvil del Expediente Digital Único en Salud.
AD-AATIC-103-2022	4 de octubre del 2022	Oficio de Advertencia referente al fortalecimiento de los mecanismos de control asociados con la premisa de garantizar la confidencialidad de la información contenida en el Expediente Digital Único en Salud (EDUS) de la Caja Costarricense del Seguro Social (CCSS).
AS-ATIC-0021-2024	7 de marzo del 2024	Oficio de Asesoría referente a la sensibilización del manejo de datos personales en el Expediente Digital Único en Salud de la Caja Costarricense del Seguro Social.

Fuente: elaboración propia, Auditoría Interna.

Por otra parte, la Contraloría General de la República mediante el informe No. DFOE-BIS-IF-00002-2022 del 20 de abril de 2022, trató el tema en el Informe “Auditoría de Carácter Especial sobre la Seguridad de la Información del Expediente Digital Único en Salud (EDUS) en la Caja Costarricense del Seguro Social”, concluyendo:

> *“El sistema EDUS es un instrumento que en efecto ha venido a fortalecer la gestión clínica de la CCSS, en favor de los usuarios de los servicios de salud, tanto a facilitar el acceso a los servicios como coadyuvando, entre otros aspectos, a la toma de decisiones, la emisión de diagnósticos y definición de tratamientos. Asimismo, ha venido a robustecer y mejorar la gestión administrativa de la institución, para procurar que la prestación de servicios se dé en forma oportuna, eficiente y eficaz.*
>
> *3.2. A pesar de lo señalado, las situaciones descritas por la Contraloría General no permiten afirmar que la gestión de la seguridad lógica del Sistema de Información (EDUS) cumple razonablemente con el marco jurídico aplicable. En ese sentido, resulta necesario gestionar los riesgos que presenta la suite de aplicaciones que conforman el EDUS, a nivel administrativo, con el fin de garantizar la seguridad de la información recopilada en los servicios de salud institucionales y cumplir el marco normativo ante el tratamiento de los datos personales.*
>
> *3.3. Asimismo, la implementación de acciones dirigidas a garantizar la aplicación de controles para la correcta asignación de perfiles de usuarios del EDUS, según las funciones y responsabilidades -actuales- de los funcionarios que atienden directamente a los usuarios de los servicios de salud, así como aquellas que permitan corregir las inconsistencias en relación con los perfiles asignados a exfuncionarios institucionales, representan medidas para fortalecer la seguridad lógica de ese sistema.*
>
> *3.4. En el tanto la CCSS logre implementar medidas para solventar los hallazgos informados, estará demostrando no solo que la gestión institucional, con respecto al sistema EDUS, se ajusta razonablemente al marco jurídico y buenas prácticas asociado a la seguridad de la información, sino también que da garantía razonable en cuanto al manejo seguro de los datos de carácter sensibles, para protegerlos de alteraciones, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado. Además, de asegurar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos contenidos en el expediente clínico.”*

V – CONSIDERACIONES FINALES

En línea con lo expuesto previamente, resulta esencial mencionar que la Administración Activa debe ser insistentes en dirigir los esfuerzos hacia una estrategia priorizada que abarque las diferentes variables interrelacionadas en esta área, incluyendo personas, procesos y tecnologías.

En ese sentido, la CCSS ostenta a futuro por avanzar hacia estos objetivos mediante la implementación de las mejores prácticas en seguridad de la información a nivel institucional. Particularmente, a través de un gobierno de datos, se podrán abordar las necesidades relacionadas con la protección de la información, identificando oportunidades de mejora y asegurando el cumplimiento normativo de manera sostenible.

Sin embargo, a corto plazo, se pueden implementar acciones para avanzar gradualmente en la cultura de seguridad, promover el monitoreo automatizado de la gestión y supervisar de manera oportuna las actividades que respaldan la prestación de servicios por parte de la Institución.

Lo anterior, a partir de las capacidades actuales de la CCSS y considerando la importancia de mitigar la exposición al riesgo mencionado en esta misiva; bajo la premisa establecida en las Normas Técnicas para la Gestión y el Control de las Tecnologías, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), específicamente en el artículo "IV. GESTIÓN DE RIESGOS TECNOLÓGICOS", al mencionar:

> *"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.*
>
> *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."*

Tal como se detalla en las observaciones de este oficio, existe el riesgo de que algunos factores estén generando inacción respecto a la justificación dada por los funcionarios de la Institución para acceder a los expedientes médicos; debilitándose los aspectos que respaldan la autodeterminación informativa y la seguridad de la información, comprometiendo la confidencialidad y la seguridad de los datos sensibles, lo cual subraya la necesidad de mejorar las medidas de control y supervisión para prevenir accesos indebidos.

Por lo tanto, es necesario fortalecer los mecanismos de control por parte de esa Gerencia en coordinación con las instancias técnicas a nivel de negocio que se encuentran involucradas, así como del apoyo tecnológico que se requiera para garantizar el cumplimiento efectivo del marco normativo relacionado a la seguridad de la información, aprovechando las oportunidades de automatización (validación de entrada de datos, notificaciones de alerta o validación de datos, analítica de datos por análisis predictivo o la visualización de datos en tiempo real, entre otras opciones) y tecnologías emergentes como sistemas de detección de anomalías (algoritmos de aprendizaje automático), la inteligencia artificial, Automatización Robótica de Procesos (RPA), entre otros requerimientos a incluir por parte de los lideres usuarios del EDUS y desarrollados por el equipo correspondiente

A ese respecto, aplicando estrategias de búsqueda de oportunidades de mejora, que incluye desde mantenerse vigilantes de las recomendaciones emitidas por los Órganos de fiscalización, entidades gubernamentales, órganos institucionales e instituciones académicas, hasta la búsqueda constante de mejoras en los procesos; sistemas de información y/o plataformas digitales; y finalmente los asuntos que refirieren a cultura, educación y ética.

Lo anterior, con el propósito de asegurar un compromiso sólido con el procesamiento justo y legal de la información, prevaleciendo la confidencialidad, integridad y disponibilidad de los datos, protegiéndolos contra cualquier uso, divulgación o modificación no autorizada, así como ante posibles daños, pérdidas u otros riesgos que puedan surgir.

En virtud de lo expuesto, esta Auditoría previene y advierte de la situación indicada en el presente oficio, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, en ese sentido, se informa a esa Administración Activa, para que realice una valoración conjunta y coordinada de los aspectos señalados, y se fortalezca las medidas de control interno en cuanto a lo expuesto, tomando las previsiones necesarias, para garantizar razonablemente en tiempo y forma del abordaje estratégico, táctico y operativo que requiere el manejo de datos personales en el Expediente Digital Único en Salud.

Se solicita comunicar, a este Órgano de Control y Fiscalización, en el **plazo de 3 meses** las acciones realizadas sobre el particular.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.07.24 13:19:38 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Máster Marta Eugenia Esquivel Rodríguez, presidente, Presidencia Ejecutiva-1102.
Máster Vilma María Campos Gómez, gerente a.i, Gerencia General -1100.
Ingeniero Esteban Zúñiga Chacón, jefe, Centro de Gestión Informática, Gerencia Médica – 2901.
Máster Robert Picado Mora, subgerente, Direccion Tecnologías de Información y Comunicaciones – 1150.
Auditoría-1111

Referencia: ID-120071