INFORME N.° **DFOE-BIS-IF-00002-2022**

20 de abril de 2022

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓNDEL EXPEDIENTE DIGITAL ÚNICO EN SALUD (EDUS) ENLA CAJA COSTARRICENSE DEL SEGURO SOCIAL

2022

Contraloría General de la República, Costa Rica
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo del Bienes Social
Auditoría Financiera - Compromiso de atestiguamiento

CONTENIDO

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

IMÁGENES

ANEXOS

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

El presente documento constituye el primer informe de la auditoría de carácter especial sobre la seguridad de la información del Expediente Digital Único en Salud (EDUS), y tuvo como objetivo determinar si la seguridad lógica de la información del Sistema EDUS cumple razonablemente con el marco jurídico aplicable. El periodo evaluado comprendió desde el 01 de enero de 2018 al 15 de febrero de 2022, el cual se extendió cuando se consideró pertinente.

¿POR QUÉ ES IMPORTANTE?

El EDUS es una plataforma digital que conceptualiza la gestión clínica para mejorar la toma de decisiones del ámbito médico, y la oportunidad, eficiencia, eficacia, calidad y acceso a los servicios de salud por parte de los usuarios. La naturaleza de los datos almacenados en el EDUS, está relacionada con información relativa al fuero íntimo de las personas, por lo cual se catalogan como datos sensibles. Así, resulta fundamental analizar si la seguridad lógica de la información se ajusta al marco jurídico y técnico aplicable, a efectos de impulsar y fortalecer las medidas técnicas y de organización para garantizar, razonablemente, la seguridad de los datos de carácter sensibles y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como su integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos contenidos en el expediente clínico.

¿QUÉ ENCONTRAMOS?

Se determinó que existen debilidades en la gestión de accesos del EDUS a lo interno de la CCSS, ante la ausencia de seguimiento e implementación de controles para administrar las cuentas de usuario de acuerdo con el cambio de estado de la relación laboral. Al respecto, al mes de noviembre de 2021, se identificó que la CCSS mantenía 14.412 perfiles habilitados para los sistemas del EDUS, asociados a 1.002 funcionarios, de los cuales 877 se encuentran jubilados y 125 son personas fallecidas. Los perfiles habilitados permitirían en el 83,73% de los casos el acceso al menos a un aplicativo de ese sistema, en 14,57% a dos, y en 1,70% hasta tres aplicativos.

También, se identificaron 1.345 funcionarios habilitados en módulos del EDUS que son utilizados para la atención directa de pacientes, cuya categoría de puesto asociado no corresponde a este tipo de perfil. De ellos, el 36% es personal financiero contable, 33% de servicios de apoyo, 9% servicios generales, 7% recursos humanos, 6% de tecnologías de información, y 9% a otros puestos no relacionados. Según el nivel de acceso que se haya asignado al usuario, estos podrían incluir nuevos datos o registros o en su defecto actualizar, modificar o consultar datos existentes. Sobre el particular, se identificó que 806 funcionarios registraron al menos un acceso a los citados módulos, entre los meses de setiembre y diciembre de 2021.

Asimismo, se determinaron 6.619 personas con permisos de acceso a módulos del EDUS que no aparecen registradas en las planillas de los meses de septiembre y octubre de 2021, lo cual no permite tener certeza con respecto a la pertinencia de los accesos brindados. También se identificaron inconsistencias en el código de Unidad Ejecutora de 100 perfiles asociados a 60 funcionarios.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Además, se identificaron riesgos de seguridad lógica, la cual resulta relevante para proteger al sistema contra ataques cibernéticos, incidentes en sistemas, bases de datos o infraestructura que pueden reducir la continuidad del servicio y comprometer la integridad, disponibilidad y confidencialidad del Expediente Digital Único en Salud, sobre los cuales no se han definido medidas específicas para su gestión.

Por último, se identificó que a la fecha de emisión de este informe, la CCSS se encontraba actualizando la documentación para continuar con la inscripción de la base de datos del Expediente Digital Único en Salud ante la Agencia de Protección de Datos de los Habitantes (Prodhab), proceso que inició desde el año 2017.

¿QUÉ SIGUE?

Se dispone a las autoridades de la CCSS, elaborar e implementar medidas para revisar todos los roles y perfiles actuales de acceso al EDUS, dar seguimiento periódico sobre su pertinencia, identificar y corregir las inconsistencias de los perfiles otorgados a los aplicativos que conforman el EDUS, y determinar la conformidad de los accesos que se realizaron.

Asimismo, la elaboración e implementación de mecanismos de control automatizados que permitan alertar y deshabilitar la cuenta de usuario de funcionarios que mantienen perfiles en los sistemas de información del EDUS una vez que se jubilen, fallezcan o finalicen su relación laboral. También, la elaboración e implementación del cronograma de medidas específicas y periódicas para gestionar los riesgos asociados a la seguridad lógica del EDUS.

Por último, se dispone la definición e implementación de medidas para concluir con el proceso de inscripción de la Base de Datos del EDUS ante la Agencia de Protección de Datos de los Habitantes (Prodhab).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA

ÁREA DE FISCALIZACIÓN DE FISCALIZACIÓN PARA EL DESARROLLO DEL BIENESTAR SOCIAL

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DEL EXPEDIENTE DIGITAL ÚNICO EN SALUD (EDUS) EN LA CAJA COSTARRICENSE DEL SEGURO SOCIAL

1. Introducción

ORIGEN DE LA AUDITORÍA

1.1. Con la promulgación de la Ley de Expediente Digital Único en Salud (EDUS), N.° 9162, del 23 de setiembre de 2013, se pretendió que todo paciente de la Caja Costarricense del Seguro Social (CCSS) dispusiera con un único repositorio digital de su información clínica, en el primer, segundo y tercer nivel de atención.

1.2. Así, el EDUS es un conjunto de sistemas de información integrados en razón de la forma en que el proceso de atención está conceptualizado, para apoyar las necesidades administrativas y de salud, tanto del paciente como de la institución. Contiene información retrospectiva, concurrente y prospectiva, y su principal propósito es soportar de manera continua, eficiente, con calidad e integridad la atención de cuidados de salud. Dicho expediente se constituye como un repositorio de los datos en formato digital y electrónico, puede ser accedido por múltiples usuarios autorizados, según el nivel de acceso asignado en diferentes establecimientos de salud.

1.3. Dada la relevancia de la información contenida en el EDUS, la cual resulta clave para la prestación de servicios de salud y la toma de decisiones de la CCSS, es importante verificar si la seguridad lógica de la información se ajusta al marco jurídico y técnico aplicable. Lo anterior, a efectos de impulsar y fortalecer las medidas de índole técnica como de organización para garantizar razonablemente la seguridad de los datos de carácter sensibles y evitar su tratamiento no autorizado, así como para asegurar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos contenidos en el expediente digital.

1.4. La auditoría se realizó en cumplimiento del Plan Anual Operativo de la DFOE y sus modificaciones, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política y los artículos 12, 17 y 21 de su Ley Orgánica, N.° 7428.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

OBJETIVOS

1.5. El propósito de la auditoría fue determinar si la seguridad lógica de la información del Sistema de Información EDUS cumple razonablemente con el marco jurídico aplicable.

ALCANCE

1.6. El presente informe abarca el análisis de la gestión de la seguridad de la información ejecutado por la CCSS con respecto al EDUS y el Módulo Integrado de Seguridad (MISE) así como el proceso de inscripción de la base de datos del EDUS ante la Prodhab. El periodo evaluado comprendió desde el 01 de enero de 2018 al 15 de febrero de 2022.

CRITERIOS DE AUDITORÍA

1.7. Los criterios de auditoría fueron comunicados mediante los oficios N.° 16292 (DFOE-BIS-0403) del 22 de octubre de 2021.

METODOLOGÍA APLICADA

1.8. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.9. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas a funcionarios de la Caja Costarricense del Seguro Social, pruebas de seguridad lógica del EDUS así como las respuestas a las consultas planteadas por escrito ante diferentes funcionarios de esa institución.

1.10. En cuanto al análisis de los perfiles de acceso habilitados en el EDUS se contó con información actualizada al 30 de noviembre de 2021, las planillas institucionales de los meses de setiembre y octubre de 2021, el detalle de los funcionarios pensionados entre el periodo del 2018 a octubre de 2021, además una base de datos de los fallecidos del Registro Civil del Tribunal Supremo de Elecciones (TSE) con corte al 31 de diciembre de 2021. Como parte del análisis, se relacionó la información de las personas registradas en la planilla con los perfiles asignados a cada usuario registrado en el MISE y con acceso a al menos uno de los diez módulos del EDUS evaluados en el estudio, así mismo se verificó cuáles de estos usuarios sesionaron en dichos sistemas durante el último cuatrimestre de 2021.

1.11. Al respecto, la CCSS habilitó un repositorio de acceso seguro para entregar los datos[1], para los cuales se veló por el cumplimiento de las "Directrices para el manejo de información de acceso restringido en la Contraloría General de la República (R-DC-75-2017)", en las que se regula el tratamiento interno de la información de acceso restringido que haya sido producida y/o se encuentre en custodia del Órgano Contralor, en ejercicio de sus funciones constitucionales y legales.

1.12. En lo concerniente al análisis de la seguridad lógica, los procedimientos efectuados se desarrollaron con un enfoque de revisión no intrusiva, el cual no generó afectación alguna de los servicios brindados por la CCSS.

[1] Correo electrónico del 9 de diciembre de 2021, referente a la coordinación de entrega y descarga de la información a través de un protocolo seguro de transferencia de archivos (SFTP).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

LIMITACIONES QUE AFECTARON LA EJECUCIÓN DE LA AUDITORÍA

1.13. La complejidad y volumen de información requerido para la ejecución de los análisis efectuados, hicieron necesaria la ampliación de los plazos para las entregas de información con respecto a los que originalmente se habían previsto en las solicitudes de información.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.14. El proyecto EDUS se declaró de interés público y nacional desde setiembre de 2013 con la Ley de Expediente Digital Único en Salud N.° 9162 y dentro de las competencias constitucionales de la Caja Costarricense del Seguro Social (CCSS), le correspondió el desarrollo de ese proyecto, el cual consiste en una plataforma digital cuyo propósito fundamental es soportar de manera continua, eficiente, con calidad e integralidad la atención de cuidados de salud.

1.15. Así, el 29 de enero de 2018 la Junta Directiva de la Caja Costarricense de Seguro Social, acordó aprobar el Reglamento del Expediente Digital Único en Salud N.° 8954, para regular la Ley N.° 9162 en protección y tutela de los derechos de la persona titular de los datos, de los integrantes del equipo técnico, profesionales en salud y de la CCSS. Además, el 13 de setiembre de 2018, la Junta Directiva en la Sesión N.° 8989 acuerda dar por atendido los plazos establecidos en la Ley 9162 para la implementación del EDUS, ante lo cual se inicia la etapa de operación del Expediente Digital Único en Salud.

1.16. El EDUS implicó desarrollar aplicativos para apoyar la prestación de servicios de salud, e integrarlos para conformar la solución informática que soporta el Expediente Digital Único de Salud. Cada aplicativo EDUS forma parte del correspondiente Sistema de Información EDUS.

1.17. El sistema de información EDUS responde a los procesos y normas asociadas con la atención ambulatoria, hospitalaria, de urgencias y servicios de apoyo en respuesta a la necesidad de los pacientes; incluye la gestión clínica y administrativa de la CCSS, la parte clínica como una forma de mejorar la toma de decisiones del ámbito médico en favor de los usuarios a través de diagnósticos certeros, detección temprana de enfermedades y tratamiento oportuno que coadyuven en una mejora de la salud de las personas mediante atención de calidad, por tanto, los registros almacenados en ese sistema de información son catalogados como datos sensibles. Por su parte, la gestión administrativa tiene como objetivo primordial mejorar la gestión general de la CCSS para garantizar que la atención de salud sea oportuna, eficiente, eficaz y de calidad.

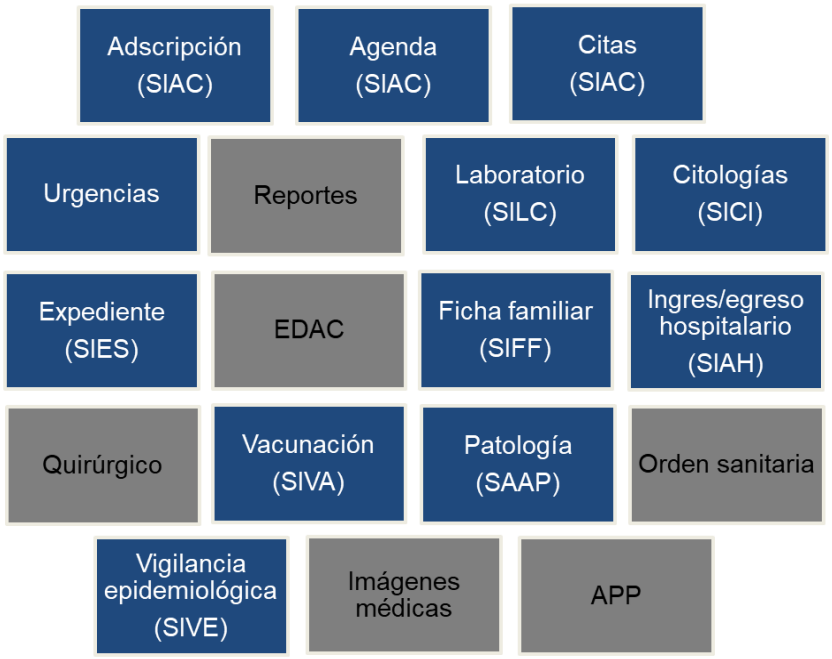
1.18. Ahora bien, los datos de la atención de cada paciente, obtenidos a través del sistema de información EDUS, se almacenan en la versión digital del Expediente de Salud, el cual incluye la información retrospectiva, concurrente y prospectiva de los usuarios. Esos datos derivados de la atención en salud o de tipo administrativo y contenidos en las bases de datos del EDUS pertenecen a la persona usuaria titular, mientras que el desarrollo y aplicativos a la CCSS.

1.19. Asimismo, los datos y la información contenidos en el EDUS son resguardados en las bases de datos dispuestas para dicho fin, las cuales no pueden ser suprimidas, modificadas o destruidas. Asimismo, los datos del EDUS sólo se pueden modificar por el proceso de atención en salud o trámite administrativo relacionado con la adscripción e identificación de los usuarios.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.20. Actualmente el EDUS dispone de 16 aplicativos en uso del personal de salud, para este estudio la información suministrada por la CCSS en cuanto a los perfiles de acceso, fue para 10 aplicativos, 43.353 personas con acceso al EDUS los cuales tienen 291.575 perfiles asignados, al 30 de noviembre de 2021, los sistemas analizados se identificaron con color azul en la imagen N.°1:

IMAGEN N.° 1 APLICATIVOS EN PRODUCCIÓN DEL SISTEMA DE INFORMACIÓN EDUS



Nota: Los aplicativos en color azul se analizaron los perfiles asignados, para los de color gris no se obtuvo información para análisis.

Fuente: Elaboración propia con base en el sistema de información EDUS.

1.21. La gestión de accesos y asignación de los perfiles requeridos, ya sea la creación, modificación o eliminación, se realiza a través del Módulo Integrado de Seguridad del EDUS (MISE) para cada aplicativo del EDUS; el nivel de autorización se asigna formalmente según la función y competencia dentro del EDUS, ya sea personal institucional o los usuarios de los servicios de salud, quienes pueden acceder a su información únicamente desde la aplicación móvil.

1.22. Además, el Reglamento del EDUS N.° 8954, establece que cada movimiento de registro, consulta, modificación, procesamiento, intercambio y almacenamiento de datos, quede consignado en el historial de seguridad del sistema así como almacenar el reporte detallado de todas las actividades desarrolladas cuyo registro no puede ser alterado, modificado, suprimido bajo ninguna circunstancia. Asimismo, obliga a todos los usuarios con acceso a los datos, a guardar la confidencialidad y el secreto profesional, aún después de finalizada la relación con el sistema de información, la CCSS o con terceros autorizados por la institución.

1.23. 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, sistemas, aplicaciones móviles y la página web institucional

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

contra accesos no autorizados, es de suma importancia en aras de evitar la posible afectación de la continuidad del servicio institucional.

1.24. Por otro lado, conviene señalar que la reglamentación emitida a la Ley N.° 9162, estableció la obligatoriedad de inscribir la base de datos del EDUS ante la Agencia Protección de Datos de los Habitantes de la República de Costa Rica (Prodhab), conforme con lo establecido en el artículo 21 de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales N.° 8968 y el artículo 44 de su Reglamento.

1.25. El proceso de inscripción requiere del formulario de solicitud acompañado de la designación del responsable y encargado de la base de datos personales ante la Prodhab y ante terceros, con la carta de aceptación del cargo y las responsabilidades inherentes al mismo, detallando el nombre, ubicación física, las finalidades y los usos previstos; los tipos de datos personales sometidos a tratamiento, los procedimientos de obtención, la descripción técnica de las medidas de seguridad que se utilizan en su tratamiento y los destinatarios de transferencias de los datos así como copia de los protocolos mínimos de actuación, el listado de los contratos globales y los medios para recibir notificaciones de la Prodhab.

1.26. Con la inscripción de la base de datos ante la Prodhab, se busca obtener los aspectos mínimos de seguridad requeridos para garantizar el adecuado tratamiento de los datos, en protección y tutela de los derechos de la persona titular, profesionales en salud y de la misma Institución, máxime que dicha agencia debe velar por el cumplimiento y resguardo de la información en las bases de datos inscritas.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.27. La comunicación preliminar de los resultados, conclusiones y disposiciones producto de la auditoría se efectuó virtualmente a las 8:00 horas del 30 de marzo de 2022, a los jerarcas institucionales, auditores internos y funcionarios de la CCSS, por medio de la herramienta Google Meet.

CONCEPTOS

1.28. Los principales conceptos utilizados en la auditoría se detallan a continuación:

Concepto	Significado
Aplicativo EDUS	Solución informática desarrollada para apoyar la prestación de servicios de salud en apego a las normas. Los aplicativos EDUS se encuentran integrados para conformar la solución informática que soporta el Expediente Digital Único de Salud. Cada aplicativo EDUS forma parte del correspondiente Sistema de Información EDUS.
Base de datos	Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso
Sistema de Información EDUS	Es un sistema de información desarrollado para facilitar la prestación de los servicios de salud y apoyar la gestión clínica y administrativa. Está constituido por un programa informático o aplicativo que responde a los procesos y normas asociadas con la atención

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

	ambulatoria, hospitalaria, de urgencias, servicios de apoyo y cualquier otra modalidad de atención que la CAJA defina en respuesta a la necesidad de los pacientes. Estos Sistemas de Información en conjunto conforman el EDUS.
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.
Datos sensibles	Los relativos al fuero íntimo de las personas o familiares, que revelen su origen étnico, opinión política, convicción religiosa o espiritual, condición socioeconómica, datos relacionados con su condición de salud o genética, vida y orientación sexual, entre otros.
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 en Salud (EDUS) Nº 9162 y el secreto profesional, principalmente cuando se acceda a información sobre datos personales, restrictos y sensibles. Esta obligación perdurará aún después de finalizada la relación con el sistema de información, con la Institución o haya terminado su relación laboral por terceros.
EDUS	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.
Integridad de los datos	Los datos contenidos en las bases de datos del EDUS, se deben considerar íntegros por la naturaleza de la información que representa, no se pueden modificar, adulterar o realizar ningún cambio, a menos que responda a un proceso de atención en salud o trámite administrativo relacionado con la adscripción, en el cual esté involucrado de manera directa el usuario de los servicios de la CAJA.
1.29. Niveles de acceso	Corresponde a los mecanismos oficiales de acceso formalmente otorgados a los usuarios del sistema, tanto administrativos como los usuarios de los servicios de salud de la CAJA, mediante acto administrativo motivado. Se determina el nivel de acceso asignado según la función realizada y competencia dentro del EDUS.
Resguardo de la información	Los datos y la información contenida en el EDUS, debe ser resguardada en las bases de datos dispuestas para dicho fin, misma que no puede ser adulterada, modificada, enajenada, suprimida o destruida parcial o totalmente. Caso contrario le será aplicada la sanción establecida en el artículo 229 bis del Código Penal y la Ley del Sistema de Archivos Nacionales.
1.30. 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

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

	propiedad de los datos contenidos en el expediente clínico.
Seguridad lógica	Se enfoca en el establecimiento de medidas de seguridad para la protección de los aplicativos, sistemas, aplicaciones móviles e incluso la página web institucional, contra accesos no autorizados que podrían afectar la continuidad del servicio.
Tratamiento de datos personales	Toda operación o conjunto de ellas, dirigida a la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, la difusión, la distribución y cualquier otra forma que facilite el acceso, el cotejo, la interconexión, el bloqueo, la supresión o la destrucción, entre otros, de los datos personales contenidos en el EDUS; efectuada mediante la utilización de hardware, software, redes, servicios, aplicaciones en el sitio o en la red u otra tecnología de la información; o incluso, mediante procedimiento manual.
Trazabilidad	El expediente digital deberá permitir llevar un registro y seguimiento de los movimientos de cada paciente, así como los suministros y recursos en los diferentes establecimientos de salud, de tal manera que dicha información se encuentre disponible para la toma decisiones, bajo los principios de confidencialidad y privacidad que para tal efecto se establezcan.
Usuario del EDUS	Persona física legitimada en razón de su función, nombramiento y/o relación con la CAJA, se incluye todos aquellos profesionales en salud en calidad de docentes, 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.
Usuario titular	Persona física usuaria de los servicios de salud que brinda la CAJA, a la cual pertenecen los datos derivados de su atención en salud o de tipo administrativo y contenidos en las bases de datos del EDUS. También titular de los datos.

SIGLAS

1.31. A continuación se detallan las siglas utilizadas en este informe:

SIGLA	Significado
APP	Aplicación informática para dispositivos móviles
CCSS	Caja Costarricense del Seguro Social
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DTIC	Dirección de Tecnologías de Información y Comunicaciones
EDAC	"Expediente Digital en Ambiente de Contingencia
EDUS	Expediente Digital Único en Salud
LGCI	Ley General de Control Interno

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

MISE	Módulo Integrado de Seguridad de la CCSS
SAAP	Sistema de Atención Anatomía Patológica
SIAC	Sistema de Identificación Agendas y Citas
SIAH	Sistema Integrado de Atención Hospitalaria
SICI	Sistema Integrado de Citología
SIES	Sistema Integrado de Expediente de Salud
SIFF	Sistema Integrado de Ficha Familiar
SILC	Sistema Integrado de Laboratorio Clínico
SINU	Sistema Integrado para los Servicios de Nutrición
SIVA	Sistema Integrado de Vacunas
SIVE	Sistema Integrado de Vigilancia Epidemiológica

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2. Resultados

2.1. Los resultados que se comunican, corresponden a temas relevantes para mantener en operación el Expediente Digital Único en Salud, así como resguardar la información de los usuarios de los servicios de salud de la CCSS. Específicamente, en lo relacionado con la gestión de permisos a los usuarios que deben acceder al EDUS, los resultados de las pruebas de seguridad realizadas y el proceso de inscripción de la base de datos ante la Agencia de Protección de Datos (Prodhab).

GESTIÓN EN LA SEGURIDAD LÓGICA DEL EDUS

DEBILIDADES EN LA GESTIÓN DE PERMISOS A USUARIOS PARA EL ACCESO A LOS SISTEMAS DEL EDUS

2.2. La CGR determinó la existencia de perfiles de acceso al sistema EDUS habilitados a personas que dejaron de ser funcionarios de la institución. Asimismo, se identificaron perfiles de acceso a aplicativos para la atención directa de pacientes, cuyos puestos y funciones sustantivas dentro de la Institución no son concordantes con los niveles de acceso designado.

2.3. De esta forma, se encontró que al mes de noviembre de 2021, la CCSS mantenía 14.412 perfiles habilitados para acceder a los sistemas del EDUS, a 1.002 personas que dejaron de trabajar para la institución o fallecieron. De estas personas, 877 corresponden a funcionarios que se acogieron a su pensión entre el 1 de enero de 2018 y el 30 de noviembre de 2021. Las restantes 125 personas corresponden a exfuncionarios fallecidos antes del 31 de diciembre de 2021.

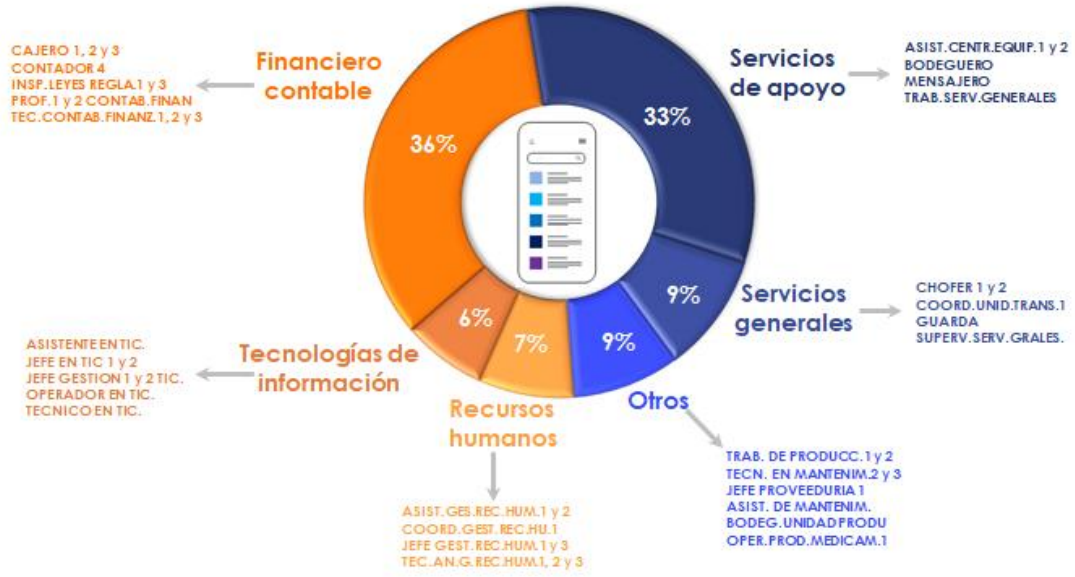
2.4. En el caso de los 877 funcionarios pensionados, estos mantenían 14.302 perfiles activos relacionados con sistemas del EDUS, a través de los cuales en el 83,81% de los casos les puede permitir acceder al menos a un aplicativo de ese sistema, el 14,60% a dos, y el 1,60% hasta tres aplicativos; en ese sentido se identificaron accesos por parte de cuatro de estos exfuncionarios en el último cuatrimestre del 2021. Además, cabe señalar que el 65,34% de esos perfiles están asociados a perfiles exclusivos o restringidos para administración de funciones de sistemas, jefatura o área específica, según lo establecido en el Anexo N.° 1.

2.5. Mientras que en el caso de las 125 personas fallecidas, los usuarios habilitados en el sistema ostentan 110 perfiles activos. Sobre el particular, al 15 de febrero de 2022, se identificó que habían transcurrido entre 59 días y 11 años desde la fecha de deceso, e incluso constató un caso donde el fallecimiento sucedió hace 61 años.

2.6. Por otra parte, se identificaron 1.345 funcionarios habilitados en módulos del EDUS para la atención directa de pacientes, cuya categoría de puesto asociado no corresponde a este tipo de perfil. De ellos, el 36% es personal financiero contable, 33% de servicios de apoyo, 9% servicios generales, 7% recursos humanos, 6% de tecnologías de información, y 9% a otros puestos no relacionados. Sobre el particular, se identificó que 806 funcionarios registraron al menos un acceso a los citados módulos, entre los meses de setiembre y diciembre de 2021. La imagen N.° 2 se detalla la distribución por cada categoría:

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

IMAGEN N.° 2 DISTRIBUCIÓN POR CATEGORÍA DE PUESTOS CON ACCESO AL EDUS



Fuente:Elaboración propia con base en los resultados de los análisis realizados.

2.7. Ahora bien, producto de la revisión efectuada, se advierte la existencia de 180.550 perfiles activos, asignados a 6.619 personas que no aparecen registradas en la planilla de los meses de septiembre y octubre de 2021, lo cual no permite tener certeza con respecto a la pertinencia de los accesos brindados. De ellos el el 77,10% al menos a un sistema, el 19,75% a dos, un 2,83% a tres y 0,24% podría acceder hasta cuatro aplicativos. Asimismo, 100 perfiles asociados 60 funcionarios cuyo código de Unidad Ejecutora está consignado como “0”, “53” o “999999”, lo cual no es consistente con el estándar institucional de cuatro dígitos.

2.8. De esta forma, la situación expuesta no es congruente con lo establecido en la norma 5.8 de las Normas de control interno del Sector Público N.° N-2-2009-CO-DFOE, en lo referente al deber del responsable de la base de datos de adoptar medidas de índole técnica y de organización necesarias para garantizar que no se den accesos no autorizados. En ese sentido, corresponde al Jerarca y los titulares subordinados, el establecimiento de controles para que los sistemas de información garanticen razonablemente la seguridad y una clara asignación de los niveles de acceso a la información y datos sensibles.

2.9. En ese sentido, Código Nacional de Tecnologías Digitales del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), establece como parte de las buenas prácticas, el mantener asignados la cantidad de privilegios mínimos, es decir únicamente los perfiles necesarios para realizar los procesos de negocio[2]. De forma similar,el

[2] Apartado de Principios del Código Nacional de Tecnologías Digitales del MICITT, del 16 de febrero de 2020.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

apartado 7.2.6 de la Guía de fundamentos para la gestión de datos[3], indica que luego de realizar un análisis cuidadoso de las necesidades de datos y responsabilidades administrativas así como el acceso limitado a los campos más confidenciales.

2.10. Por su parte, los apartados 8.1.4.3 y 8.1.5.8 del Manual operativo del Reglamento del EDUS[4], establecen los pasos que deben seguir los funcionarios responsables para gestionar y autorizar las solicitudes de creación, modificación, cambio de estado, la temporalidad, asignación o reasignación de perfiles de las cuentas de los Administradores Locales y Usuarios Finales en el Módulo Integrado de Seguridad (MISE). Asimismo, señala que en el caso de puestos en propiedad el plazo debe ser de dos años y en los interino por el periodo del nombramiento o cambio de funciones.

2.11. Además, el citado Manual Operativo, en los Apartados 8.1.6.1, 8.1.6.6 y 8.1.6.7, establece el deber de los funcionarios asignados de revisar y tramitar las solicitudes de creación, modificación, cambio de estado, de los Administradores Locales y Usuarios Finales en el MISE, por cada aplicativo del EDUS. También el implementar procedimientos y mecanismos de control, evaluación y seguimiento periódico para fortalecer la gestión de las cuentas de accesos a los sistemas de información del EDUS.

2.12. A su vez, los apartados 9.3.2.a), 9.3.2.b) y 9.3.3 de dicho Manual señalan que cuando el funcionario cambie su estatus por finalización del contrato laboral, jubilación o fallecimiento, vacaciones, incapacidad, licencia, permiso con o sin goce de salario, cambio de perfil laboral en forma temporal o permanente, se deberá suspender o deshabilitar la cuenta de usuario con vigencia en su fecha de caducidad. En ese sentido, la Guía de Perfiles de Acceso por aplicativo del EDUS, indica que se deben agregar o deshabilitar un perfil a la cuenta de un usuario, de acuerdo con las funciones que realiza en el servicio o unidad donde labora.

2.13. Las situaciones señaladas obedecen a la ausencia de seguimiento e implementación de los controles, para bloquear o deshabilitar la cuenta de usuario cuando el funcionario cambia su estatus por finalización del contrato laboral, jubilación o fallecimiento y se garantice la revisión periódica así como los ajustes pertinentes de los accesos asignados para minimizar el riesgo de perfiles indebidos por cambios en la condición laboral. Aunado a ello, la Administración señaló que en el MISE no se integra la gestión de movimientos de personal, por lo cual puede omitirse la consideración de eventuales ascensos de funcionarios o ejecución de tiempos extra.

2.14. En consecuencia se potencia el riesgo de seguridad y tratamiento inadecuado de los datos personales y sensibles -de los usuarios de los servicios de salud- almacenados en el EDUS, cuya materialización podría comprometer la imagen de la CCSS y acarrear eventuales sanciones administrativas, legales y financieras. Así como el riesgo de fuga de los datos personales y sensibles administrados en la CCSS a través del EDUS, los cuales podrían ser utilizados con fines distintos para lo cual se recabaron.

DEBILIDADES EN LA SEGURIDAD LÓGICA DEL EDUS

2.15. La Contraloría General identificó riesgos de seguridad lógica que pueden comprometer la integridad, disponibilidad y confidencialidad del Expediente Digital Único en Salud. El

[3] Guía de fundamentos para la gestión de datos, Global Data Management Community (DAMA), 2010.

[4] Manual operativo del Reglamento del EDUS N.° GM-AES-MO-01 Versión 00.02 de febrero 2019.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

detalle de los riesgos identificados se comunicaron a la Caja Costarricense de Seguro Social mediante oficio N.° 4768 (DFOE-BIS-0189) del 21 de marzo de 2022[5].

2.16. En cuanto al manejo de las debilidades identificadas, la ley Expediente Digital Único de Salud, N.° 9162, señala en el artículo 11 que 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, incluyendo, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual y que permita proteger de la información almacenada.

2.17. Al respecto, el Código Nacional de Tecnologías Digitales del MICITT, establece en el capítulo 3 que a nivel de ciberseguridad la infraestructura tecnológica debe contar con procedimientos para el inventario y descubrimiento de activos tecnológicos necesarios para la operación de la organización. Además, refiere al deber de administrar esa infraestructura desarrollando procedimientos para la actualización frecuente de firmware, controladores y parches del sistema operativo, aplicaciones y dispositivos, así como que el desarrollo de la ciberseguridad en la infraestructura tecnológica debe de contar con un inventario de software oficial y actualizado periódicamente.

2.18. También, el citado Código señala que el acceso a los activos físicos y lógicos e instalaciones asociadas debe estar limitado a los usuarios, procesos y dispositivos autorizados, que los mecanismos de autenticación deben garantizar la veracidad de la identidad del usuario y seguir las mejores prácticas para prevenir el mal uso o el abuso por parte de usuarios o sistemas no autorizados.

2.19. Además, sugiere el uso de criptografía para información de acceso restringido y el desarrollo de la ciberseguridad, así como la validación, filtrado y codificación, la información recibida por las aplicaciones, para prevenir la posibilidad de envío de información maliciosa.

2.20. Sobre el particular, la norma ISO 27001, sobre Gestión de Seguridad de la Información, en su cláusula A.8.2.1, indica que para la gestión de la seguridad de la información, la información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

2.21. Ahora bien, las debilidades encontradas con respecto a la seguridad lógica, obedecen a que la CCSS no ha definido las medidas específicas para gestionar los riesgos comunicados por la Contraloría General; lo cual potencia el riesgo de accesos no autorizados, pérdida o modificación de información y degradación parcial o total de los servicios.

2.22. Además, se expone el sistema a ataques de denegación de servicios, y se puede comprometer la seguridad del software con la eventual obtención de privilegios de administrador para acceder a información confidencial, así como ejecutar comandos para copiar, eliminar o modificar archivos o bases de datos.

ATRASOS EN EL PROCESO DE INSCRIPCIÓN DE LA BASE DE DATOS

2.23. Se encontró que desde el año 2017 la CCSS inició las gestiones para inscribir la base de datos del Expediente Digital Único en Salud ante la Agencia de Protección de Datos de los Habitantes (Prodhab); sin embargo a la fecha de emisión de este informe dicho

[5] Oficio declarado confidencial por la naturaleza de su contenido.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

proceso no ha concluido. En ese sentido el proceso inscripción conlleva la elaboración de protocolos mínimos de actuación, medidas de seguridad que se utilizarán en el tratamiento de los datos personales, designación del responsable y encargado de la base de datos[6].

2.24. Estos protocolos y medidas de seguridad son relevantes por cuanto requieren del establecimiento, mantenimiento y revisión de medidas administrativas, físicas y lógicas dirigidas a asegurar razonablemente la protección de los datos personales y sensibles de los usuarios de los servicios de salud. La implementación de lo anterior, representa un garante adicional, para el manejo seguro de la información, de acuerdo con lo establecido en el Reglamento del EDUS N.° 8954, así como en la Ley de Protección de la Persona frente al tratamiento de sus datos personales N.° 8968 y su reglamento.

2.25. Sobre el particular, según lo establecido en el artículo 48 del Reglamento del Expediente Digital Único en Salud[7], la inscripción de de la base de datos del EDUS ante la Prodhab, le fue asignada a las Gerencias Médica y de Infraestructura y Tecnologías, en función de lo establecido en el artículo 21 de la Ley N.° 8968[8].

2.26. En ese sentido, la Ley del Expediente digital único de salud N.° 9162, establece en el artículo 11 que 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, así como la pérdida, tratamiento o acceso no autorizado.

2.27. La situación descrita obedece a que las acciones ejecutadas por la Gerencias Médica y de Infraestructura y Tecnologías, han sido insuficientes para concluir la inscripción de la Base de datos ante la Prodhab, conforme a los requisitos establecidos en el artículo 44 del Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, responsabilidad asignada desde el año 2018. A la fecha de emisión del presente informe, la institución se encontraba actualizando la documentación que debe acompañar el formulario de solicitud para continuar con la inscripción ante la Prodhab[9].

2.28. De esta forma, lo señalado potencia el riesgo de no garantizar que los datos personales y sensibles contenidos en el EDUS se traten bajo las medidas de índole técnica y de organización necesarias, definidas normativamente por la CCSS.

[6] Artículo 44 del Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Decreto Ejecutivo N.° 37554 del 30 de octubre de 2012.
[7] Aprobado por la Junta Directiva de la CCSS en el artículo 4 de la sesión N.° 8954. Publicado el 20 de febrero de 2018.
[8] Artículo 21. Registro de archivos y bases de datos. “Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasbase o la transferencia de los datos”.
[9] Oficio N.° GM-AES-1-0449-2022 del 14 de marzo de 2022.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

3. Conclusiones

3.1. El 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.

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, N.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los “Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría”, emitidos mediante resolución N.° R-DC-144-2015, publicados en La Gaceta N.°

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

AL DOCTOR RANDALL ÁLVAREZ JUÁREZ, EN SU CALIDAD DE GERENTE MÉDICO O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Definir e implementar medidas específicas para: a) revisar la asignación de roles y perfiles de los aplicativos del EDUS asignadas a los funcionarios cuya categoría de puesto no es correspondiente con perfiles de atención directa de pacientes, así como para dar seguimiento periódico sobre su pertinencia, b) corregir las inconsistencias entre el perfil asignado y la categoría de puesto, c) determinar si se dieron accesos a información protegida por ley a través de los perfiles que fueran incorrectamente asignados, y d) instruir los procedimientos conforme a derecho corresponda para los casos que se identifiquen. Remitir a la Contraloría General una certificación que acredite la definición de las medidas, a más tardar el 30 de junio de 2022. Además, dos certificaciones que acrediten el avance en la implementación a más tardar al 16 de setiembre de 2022 y al 16 de enero de 2023. (Ver párrafos del 2.2 al 2.13).

AL DOCTOR RANDALL ÁLVAREZ JUÁREZ, EN SU CALIDAD DE GERENTE MÉDICO Y MÁSTER ROBERTO BLANCO TOPPING, SUB GERENTE A.I. DE TECNOLOGÍAS Y COMUNICACIONES O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.5. Elaborar, divulgar e implementar mecanismos de control automatizados que permitan alertar y deshabilitar los perfiles de los usuarios en los sistemas de información del EDUS y las soluciones de inteligencia de negocios asociadas a la atención directa de pacientes, una vez que los funcionarios se jubilen, fallezcan o finalicen su relación laboral. Remitir a la Contraloría General, a más tardar el 30 de noviembre del 2022, una certificación que acredite que dichos mecanismos fueron elaborados y divulgados. Asimismo, una certificación a más tardar el 30 de junio de 2023, que haga constar el avance en la implementación de los mecanismos. (Ver párrafos del 2.2 al 2.13).

AL SEÑOR ROBERTO BLANCO TOPPING EN SU CALIDAD DE SUBGERENTE A.I. DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.6. Elaborar e implementar el cronograma de las medidas específicas para gestionar los riesgos asociados a la seguridad lógica del Expediente Digital Único en Salud, así como asegurar que la remediación cumpla con las mejores prácticas. Dicho cronograma debe considerar al menos las medidas específicas, fecha y responsable de implementarlas. Remitir a la Contraloría General de la República, una certificación en la cual se acredite la elaboración del cronograma para gestionar los riesgos que le fueran comunicados en el oficio N.° 4768 (DFOE-BIS-0189), a más tardar el 31 de mayo de 2022; así como una certificación de avance en la implementación del cronograma a más tardar el 30 de setiembre de 2022. (Ver párrafos del 2.14 al 2.21).

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

AL DOCTOR ROBERTO CERVANTES BARRANTES, GERENTE GENERAL, Y AL DOCTOR RANDALL ÁLVAREZ JUÁREZ, GERENTE MÉDICO O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.7. Definir e implementar las medidas para concluir el proceso de inscripción de la base de datos del EDUS ante la Agencia de Protección de Datos de los Habitantes (Prodhab), de conformidad con lo establecido en el marco normativo atinente. Remitir a la Contraloría General una certificación que haga constar la definición de las medidas tomadas a más tardar el 31 de mayo de 2022. Además, una certificación que acredite el avance en la implementación de las medidas al 31 de octubre de 2022. (Ver párrafos del 2.22 al 2.27).

Firmado digitalmente por MANUEL JESUS CORRALES UMAÑA
Fecha: 2022-04-20 11:41

Lic. Manuel Corrales Umaña, MBA

Gerente de Área

Firmado digitalmente por MARVIN MEJIA VARGAS
Fecha: 2022-04-20 11:34

Lic. Marvin Mejía Vargas, MSc.

Asistente Técnico

Firmado digitalmente por KENNETH IRVIN MONGE QUIROS
Fecha: 2022-04-20 11:20

MSc. Kenneth Irvin Monge Quiros.

Coordinador

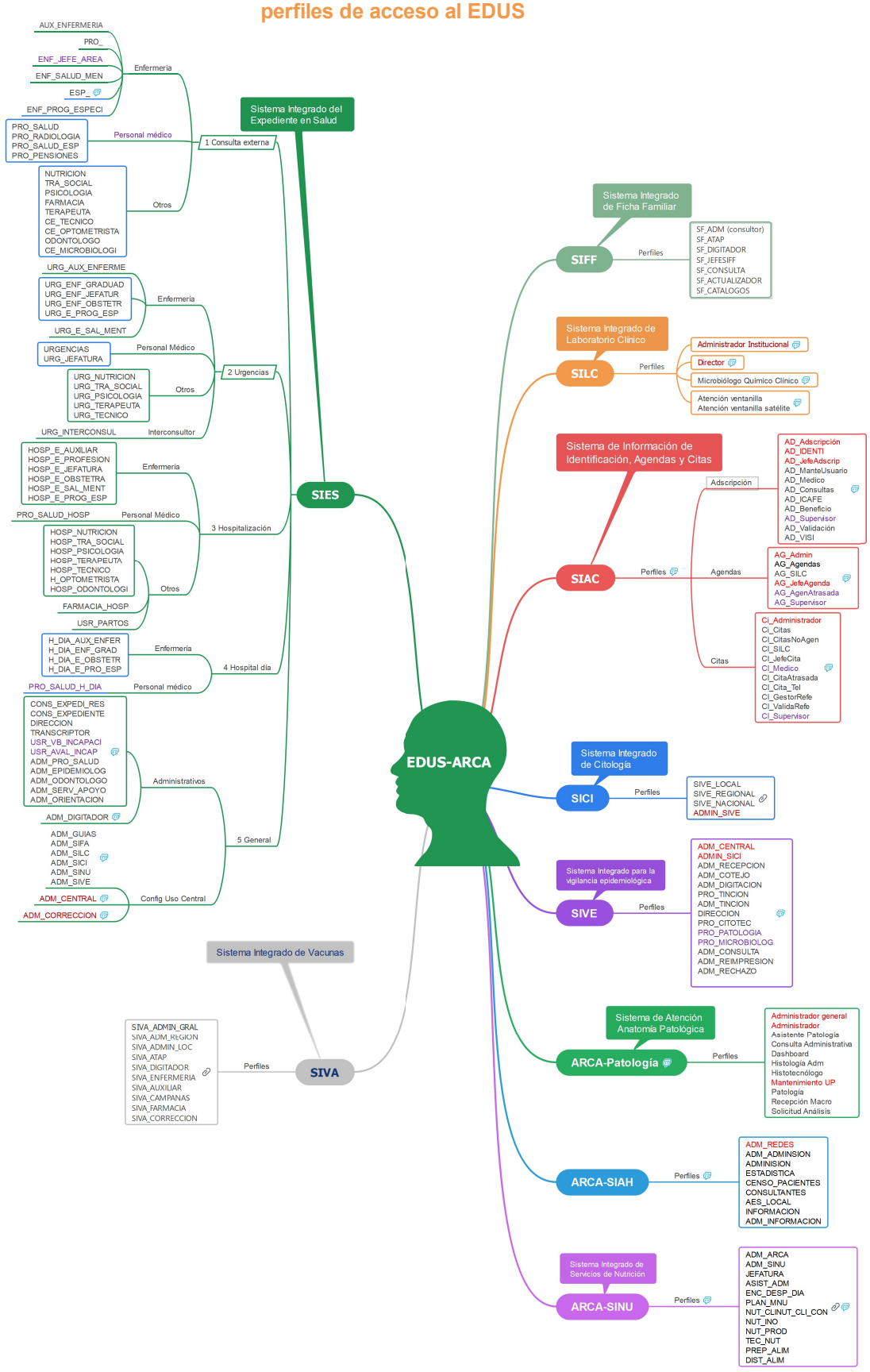
Firmado digitalmente por VIRIA MELISSA RODRIGUEZ SALAS
Fecha: 2022-04-20 11:24

Licda. Viria Melissa Rodríguez Salas

Colaborador

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo N.°1 Análisis de los perfiles de acceso al EDUS



NOTA: Los perfiles con fuente color rojo son exclusivos o restringidos para: administración de funciones de sistemas, jefatura o área específica.

Fuente: Elaboración propia con base en las guías rápidas y manuales de gestión de perfiles del EDUS