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

Al contestar refiérase a: **ID-110253**

AS-ATIC-0021-2024
7 de marzo de 2024

Doctor
Wilburg Díaz Cruz, gerente a.i

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

Estimado(a) señor(a):

ASUNTO: **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.**

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 asesoría referente a la sensibilización del manejo de datos personales en el Expediente Digital Único en Salud (EDUS) de la Caja Costarricense del Seguro Social (CCSS), 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."*

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.

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"*

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.***

III- PRODUCTOS DE FISCALIZACIÓN RELACIONADOS AL TEMA

Sobre el particular, esté Órgano Fiscalizador ha emitido tres productos que refieren concretamente a temas relacionados con la protección de la persona frente al tratamiento de sus datos personales y sobre el aplicativo móvil del Expediente Digital Único en Salud, 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).

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."

IV- OBSERVACIONES

Según lo establecido en la ley No. 8968, la información administrada a través del EDUS comprende datos personales, al caracterizarse por identificar a una persona física, en este caso que accede a los servicios médicos de la Institución.

En particular, una parte de estos datos personales se clasifican como sensibles, lo cual conlleva que estén sujetos a todas las disposiciones de privacidad y restricciones de tratamiento requeridas por la normativa vigente.

Para tales efectos, se presentan las siguientes observaciones que podrán ser valoradas en esa Administración para diseñar, implementar o mejorar las estrategias asociadas a la temática de marras.

- **Divulgación de la información:** Se debe recordar a los funcionarios que, por la naturaleza de su labor en la cadena de servicio, pueden estar expuestos a cierta información inherente a la atención médica recibida por el usuario.

  Sin embargo, los datos de su conocimiento deben ser utilizados estrictamente con fines estadísticos y desvinculados de la identidad de la persona, a menos que el titular haya otorgado un consentimiento previo y válido para su divulgación.

  Lo anterior, complementando y ampliando el esfuerzo dado para oficializar el "Manual Operativo Desasociación y Anonimización de datos personales de la persona usuaria en la Caja Costarricense de Seguro Social, Código: GM-AES-MO-20", versión 01, diciembre 2023, de aplicación obligatoria, para todos aquellos usuarios EDUS en los tres niveles de atención o terceros autorizados con quien la CCSS haya suscrito convenio, contrato u otra forma de relación legítima, incluidos los establecimientos de salud administrados por proveedores externos, que en su ámbito de competencias deban realizar acciones de recolección, registro, conservación, extracción, consulta y utilización de los datos personales que se encuentran en las bases de datos EDUS/ARCA y la protección a la privacidad de la información de la persona usuaria

- **Responsabilidad de los funcionarios:** es crucial que cada centro de salud de la CCSS y sus funcionarios estén plenamente conscientes de la importancia de mantener el secreto profesional inherente a su labor. Esto implica no solo salvaguardar la información personal, la privacidad y la confidencialidad de los pacientes que acceden a los servicios de la Institución, sino también cumplir con el deber ético de protegerla.

  En otras palabras, teniendo en cuenta que la responsabilidad de mantener la confidencialidad de cualquier persona diagnosticada con una condición médica se extiende a todos los ciudadanos.

- **Socialización de los canales para interponer denuncias:** Con el propósito de facilitar a la población (interesado en el tratamiento de sus datos personales) la obtención de información necesaria para proceder a denunciar la vulneración de sus derechos de privacidad, se debe fortalecer la transparencia y la confianza en el sistema.

  A ese respecto, la divulgación clara y accesible de los medios disponibles para exponer las posibles violaciones a los datos personales, así como los requisitos mínimos necesarios para respaldar una investigación adecuada, resulta crucial para asegurar la efectividad y legitimidad de los procesos relacionados con este tema.

  Lo anterior, complementando y ampliando el esfuerzo dado para oficializar la “Guía para operacionalizar el procedimiento de notificación, gestión y respuesta de accesos indebidos en el Expediente Digital Único de Salud”, versión 01, noviembre 2023, aplicable a funcionarios, así como terceros autorizados mediante convenio, contrato u otra forma de relación legítima con la CCSS; entre otra normativa que refiere a los proceso de acceso a la información por parte de la persona usuaria titular de los datos o representante legal.

- **Sobre el Curso “Sensibilización en la Seguridad de la Información, Protección y Tratamiento de Datos Personales en el EDUS:** El pasado 5 de febrero de 2024, como se comunicó en la Webmaster, la declaración de interés institucional asociada al Curso de *"Sensibilización en Seguridad de la Información, Protección y Tratamiento de Datos Personales en el EDUS".* A partir de esa notificación, la decisión de participar queda a discreción del funcionario y su respectiva jefatura.

  Sin embargo, es de destacar que la participación en este tipo de actividades debe ser deliberada y cuidadosamente planificada para asegurar el cumplimiento de los objetivos, como de la asistencia razonable de la población meta, dadas las responsabilidades directamente relacionadas con los temas propuestos.

  En ese sentido, se sugiere que en futuras actividades se tenga en cuenta el público objetivo, considerando la naturaleza de sus funciones y la necesidad especifica de participar.

- **Vigencia de las observaciones del oficio de advertencia AD-AATIC-103-2022:** Esta Auditoría Interna emitió el oficio AD-AATIC-103-2022, destacando los siguientes aspectos:

  - Generación de alertas para advertir sobre situaciones fuera de patrones predeterminados, acciones sospechosas o justificaciones improcedentes para acceder a información sensible.

  - Incentivar la protección de datos mediante técnicas de supervisión, vinculadas con el cumplimiento de procedimientos y marco normativo vigente; principalmente aplicada a las justificaciones dadas al acceder a la información sensible del EDUS.

  - Invertir esfuerzos en la gestión de requerimientos orientada a promover la mejora continua en el manejo del expediente digital y sus implicaciones, impulsada por líderes de proceso que posean un profundo conocimiento del contexto de la CCSS y estén al tanto de las eventualidades operativas relacionadas con los datos.

  - Concientización de los usuarios apoyado en la capacitación y entrenamiento, considerando el perfil de acceso en el EDUS y/o manejo que tenga este de datos sensibles en el expediente digital.

  Como se puede observar, los temas abordados en la misiva siguen siendo relevantes y constituyen aspectos que deben ser monitoreados de manera continua en busca de oportunidades de mejora. Es decir, aunque pudieran haber sido analizados en un momento específico y considerarse resueltos, es fundamental revaluar las observaciones periódicamente, en aras de fortalecer los procedimientos vinculados a cada asunto.

- **Alcance de los protocolos para el manejo de datos personales:** resulta indispensable verificar de manera periódica los protocolos de tratamiento de datos personales y las medidas de seguridad en aras de que sean integrales y/o se interrelacionen, en virtud de la cantidad de actividades y personas que participan desde el momento en el cual la persona usuaria se somete a: solicitar cita médica, consulta médica, exámenes clínicos, ser diagnosticado, recibir prescripción de tratamiento farmacológico, otorgamiento de incapacidades, vigilancia epidemiológica, trámites de índole administrativa; e incluso al resguardo de la información, generación de estadísticas, investigación biomédica, reportes en función de la salud pública, entre otros procesos.

- **Evolución de sistemas de información y modalidades de atención:** Ante la rápida evolución en las formas de atención médica, incluyendo las características para el abordaje al usuario, por ejemplo: telemedicina, consultas vía telefónica, interoperabilidad de sistemas de información, integración de equipamiento médico, entre otras tecnologías emergentes, es fundamental reiterar la importancia de otorgar un tratamiento responsable a los datos personales en general, y de manera particular, a la información sensible.

V – CONSIDERACION FINAL

En línea con lo expuesto previamente, resulta esencial dirigir los esfuerzos hacia una estrategia integral que abarque las diferentes variables interrelacionadas en esta área, incluyendo personas, procesos y tecnologías; entre las iniciativas a desarrollar para conseguir resultados asociados con esa premisa, se sugiere que esa Gerencia pueda coordinar con la Dirección de Comunicación Organizacional para obtener respaldo en el diseño de campañas de divulgación masiva dirigidas a funcionarios con acceso a la información sensible gestionada en el expediente clínico, bajo el propósito de concientizar al conjunto de involucrados sobre el deber de cuidado y responsabilidad establecida por las leyes y regulaciones pertinentes en materia de protección y privacidad de datos.

En ese sentido, la CCSS ostenta alcanzar estos aspectos mediante la implementación de las mejores prácticas relacionadas con la seguridad de la información a nivel institucional, siendo uno de los principales desafíos en este ámbito es la creación de cultura. Particularmente, a través de un gobierno de datos, será posible abordar la mayor cantidad de necesidades vinculadas con la protección de la información, brindando oportunidades de mejora y garantizando posteriormente el cumplimiento normativo de manera sostenible.

Sin embargo, según las capacidades actuales de la Institución, es posible mitigar la exposición al riesgo y ejercer un control efectivo sobre el ciclo de vida de la información personal de los usuarios del seguro de salud, considerando entre otras las observaciones inmersas en este oficio.

Lo anterior, 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.”*

A ese respecto, se podría fortalecer las habilidades de los funcionarios de la Institución en lo referente al manejo de datos, asegurando que se adhieran a los principios éticos afines al procesamiento justo y legal de la información. Esto implica garantizar con un compromiso sólido, la confidencialidad, integridad y disponibilidad que

se le brinde a esta, protegiéndola contra cualquier uso; divulgación o modificación no autorizada; posibles daños; pérdidas u otros riesgos que puedan surgir.

Esto se lograría a través de la socialización permanente de los protocolos que eviten la divulgación de datos personales; generando conciencia en la responsabilidad de los funcionarios y brindando capacitación, sobre sus deberes en el desarrollo de funciones.

En adición a la constante búsqueda de oportunidades de mejora, que incluye desde mantenerse vigilantes de las recomendaciones emitidas por entes de fiscalización tales como las mencionadas en el oficio de advertencia AD-AATIC-103-2022, así como de entidades gubernamentales, órganos institucionales e instituciones académicas; socializar los canales para interponer denuncias; hasta velar por el cumplimiento normativo frente a las tecnologías emergentes, las cuales a menudo, se pasa por alto los riesgos y las implicaciones asociadas al tratamiento de datos.

Debido a lo anterior, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a esa gerencia, para que realice una valoración de los aspectos señalados, a efectos de que se concreten a la brevedad posible las acciones necesarias para el abordaje en el ámbito estratégico, táctico y operativo del manejo de datos personales en el Expediente Digital Único en Salud.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.03.12 11:56:28 -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 Campos Gómez, gerente a.i, Gerencia General - 1100.
Auditoría-1111

Referencia: ID-110253