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

AS-AATIC-175-2022
17 de agosto de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA - 2901

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA - 1103

Licenciado
Luis Fernando Campos, gerente
GERENCIA ADMINISTRATIVA - 1104

Doctor
Esteban Vega de la O, gerente
GERENCIA DE LOGÍSTICA - 1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS - 1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES – 9108

Estimados señores:

ASUNTO:	**Oficio de Asesoría relacionado con los Sistemas de Gestión de Privacidad de la Información en el contexto actual de la Caja Costarricense de Seguro Social.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y
con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, específicamente en su rol de asesor, esta Auditoría informa sobre los mecanismos y acciones que permiten un mayor fortalecimiento en la gestión de la privacidad de los datos que se administran en los diferentes sistemas institucionales, con el objetivo de generar un tratamiento adecuado de la información de los usuarios en apego al marco jurídico vigente y que tenga como efecto la disminución de la materialización de riesgos relacionados con esta temática.

Al respecto, la Institución en los últimos años se ha encontrado un proceso de transformación digital tanto de los servicios que se brindan a la población como de las diferentes gestiones administrativas que se realizan a lo interno, esto ha generado que mucha información sensible de carácter privado sea gestionada mediante los diferentes sistemas institucionales, los cuales fueron creados con el fin de mejorar la eficiencia y eficacia de la gestión de la información mediante el procesamiento de los datos. No obstante este proceso de transformación digital se ha tenido que detener momentáneamente ante el ataque cibernético sufrido el pasado 31 de mayo, generando un impacto en los procesos institucionales, y creando la necesidad de llevar estos manualmente con el fin de continuar con la prestación de los servicios y que el usuario sufra la menor afectación posible, lo que va a conllevar que posteriormente y una vez normalizada la plataforma tecnológica institucional, se genere un proceso de inclusión de la información a los diferentes sistemas de la Caja donde se debe asegurar la seguridad del tratamiento de los datos y su integridad.

Por lo anterior, considera esta Auditoría que es importante que, dentro de sus diversas estrategias, la Institución analice la viabilidad de la implementación de sistemas de gestión de privacidad de la información ofreciendo la posibilidad de evidenciar a la población un cumplimiento efectivo de las normativas de protección de datos, generando confianza, protegiendo la reputación de la Institución y protegiéndose de la responsabilidad legal y sancionatoria que se puede generar por el incumplimiento de normas como la Ley de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales.

Al respecto, la International Organization for Standarization, conocida como ISO, junto con la International Electrotechnical Commission o EIC, han creado una serie de estándares de seguridad de la información como la ISO 27000 y la norma ISO 27701 la cual se convirtió en una norma internacional de referencia para gestionar y garantizar la seguridad de la información en empresas y organizaciones

La ISO 27701 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad (PIMS por sus siglas en inglés), la misma está basada en los requisitos, controles y objetivos de la norma ISO 27001: Requisitos de Sistemas de Gestión de Seguridad de la Información (SGSI). Dicho estándar ayuda a reducir los riesgos de privacidad en los tratamientos de datos personales o información de identificación personal (PII) aportando garantías de seguridad sobre los tratamientos de los datos personales, incorporando la gestión de la privacidad en la gestión de riesgos de la Organización, controlando la existencia de mecanismos para la notificación de brechas de privacidad, estableciendo roles y responsabilidades claras sobre los tratamientos de la información, mejorando la gestión de contratos con los encargados, verificando el registro de actividades, contribuyendo a implementar la privacidad por diseño y por defecto en los tratamientos y garantizando que se permita a los propietarios de los datos personales, el ejercicio de sus derechos sobre los mismos.

En concordancia con lo anterior, la implementación de un sistema de Gestión de Privacidad de la Información genera múltiples beneficios entre los que se encuentran:

- Genera confianza.
- Permite certificar el cumplimiento de las prácticas en materia de gestión de datos de carácter personal dentro de la organización.
- Apoya el trabajo colaborativo.
- Proporciona transparencia entre las partes interesadas.
- Ayuda a mejorar los procesos de gestión de la información de carácter personal.

- Aclara roles y responsabilidades.
- Aumenta la responsabilidad de la Organización en el tratamiento de datos y en la seguridad de información de identificación personal.
- Facilita acuerdos comerciales efectivos.
- Ayuda a cumplir con el marco jurídico relacionado con la protección de datos.

Entre las características que presenta el estándar ISO 27701, es la definición de la Información de Identificación de Personal o PII que corresponde a los datos personales que se manejan en los diferentes sistemas de la Organización, asimismo detalla dos actores importantes: el Controlador de PII o controlador de datos y el Procesador de PII o procesador de datos que entre sus características se detallan los siguientes:

- Las personas autorizadas para acceder a la Información de Identificación de Personal IIP, deben firmar y aceptar un acuerdo de confidencialidad.
- La norma exige realizar una evaluación de riegos de privacidad, para identificar amenazas de procesamiento de PII.
- Las Organizaciones deben designar personas responsables de desarrollar, implementar, mantener, monitorear, evaluar y mejorar el Sistema de Gestión de Seguridad de la Información.
- Es preciso identificar las necesidades de capacitación y proporcionar los programas adecuados a los empleados que tienen acceso a PII.
- La organización debe adoptar políticas y procedimientos, así como planes de respuesta a incidentes de violaciones de PII.
- La norma solicita a las organizaciones mantener registros de todas las actividades de procesamiento de PII, incluidas las transferencias entre diferentes jurisdicciones y la divulgación a terceros.

Al respecto la Ley 8969 “Protección de la Persona frente al tratamiento de sus datos personales” en el artículo 10 “Seguridad de los datos” señala:

> *“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, así como cualquier otra acción contraria a esta ley.*
>
> *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.*
>
> *No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. (…)”.*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la “Arquitectura Empresarial”, señala:

"La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información (…).

(…) La institución debe disponer de un modelo de clasificación de datos e información, según criterios y requisitos legales, de valor, según el nivel de criticidad y susceptibilidad a divulgación o modificación no autorizada. La Unidad de TI se basará en este modelo para establecer las directrices de seguridad y protección de los datos e información institucionales."

En virtud de lo expuesto, se da conocer la información descrita, con el propósito que sea sometida a valoración y revisión por esa Administración y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional, así como del cumplimiento de la normativa legal y técnica, especialmente en el tratamiento de datos personales, que puedan generar a la Institución inconvenientes ante la materialización de los riesgos señalados, por esta razón considera esta Auditoría es importante se efectúe un análisis y se valoren las medidas correspondientes para garantizar que tanto los sistemas de información en funcionamiento actualmente, como las contingencias utilizadas por las unidades en medio de la emergencia por el ataque cibernético, cumplan con el objetivo de generar eficiencia y eficacia en los servicios prestados, sin que se vulneren los derechos de los usuarios.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.08.17 21:08:04 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

C. Máster Idannia Mata Serrano, subgerente a.i., Dirección de Tecnologías de Información y Comunicaciones - 1150.
Auditoría