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

AS-AATIC-107-2022
22 de junio 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 LOGÍSTICA - 1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍA - 1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES - 9108

Estimados señores:

ASUNTO:	**Oficio de Asesoría referente al tratamiento de los datos personales y medidas de seguridad.**

Esta Auditoría, en cumplimiento de las actividades preventivas y de asesoría consignadas en el Plan Anual Operativo, para el período 2022 y con fundamento en lo dispuesto en los artículos 21 y 22 de la Ley General de Control Interno, informa sobre el tratamiento de los datos personales y las medidas de seguridad como consecuencia de los ataques cibernéticos generados a la institución, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa Administración.

ANTECEDENTES

El 9 de marzo 2022, mediante oficio GG-DTIC-1368-2022, la Dirección de Tecnologías de Información y Comunicaciones, informó sobre incidencia que se presentó el 7 de marzo 2022 a las 8:06 a.m., en equipos de seguridad por tráfico anómalo, lo cual provocó alto tráfico y lentitud en la infraestructura tecnológica, los sistemas impactados fueron EDUS, SICERE y la autenticación de redes virtuales privadas (VPN).

El 19 de abril 2022, fue el turno de la cuenta Twitter de la CCSS, así lo publicó ese día el diario La República, en nota titulada "*Hackeo a cuenta de Twitter de la CCSS y sitio alterno del Micitt se unen al del Ministerio de Hacienda"*.

El 20 de abril 2022, el portal de Recursos Humanos sufrió un ataque cibernético por parte de hackers del grupo Conti, tal como lo informó el diario La Nación esa misma fecha, en nota con el titular de "*Portal de Recursos Humanos de CCSS sufre ataque cibernético*", indicando:

> *"Las plataformas digitales de las entidades públicas siguen siendo objeto de ataques cibernéticos. La Caja Costarricense de Seguro Social (CCSS) sufrió este miércoles una incidencia en su portal de Recursos Humanos, que obligó a activar una revisión integral de todos sus sistemas para determinar el alcance de lo ocurrido.*
>
> *El ingeniero Roberto Blanco Topping, director de Tecnologías de Información de la CCSS, detalló que una vez detectado el problema se procedió a blindar los accesos, dar de baja el portal y coordinar con los equipos técnicos para determinar si se produjo alguna extracción de información o de datos, o eventuales accesos a otras plataformas".*

Asimismo, el 31 de mayo 2022, en horas de la madrugada se registró un nuevo evento, esta vez contra la infraestructura de telecomunicaciones (redes LAN y WIFI, muchas de ellas deshabilitadas con el fin de evitar la propagación del virus) y servidores de la Caja (Active Directory, SCCM, DHCP, DNS, en su mayoría afectados sin opción de rescate más que el formateo y reinstalación), el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

Fue así como el diario La República publicó el 31 de mayo 2022, "*Hackers tenían como objetivo el robo de información y las bases de datos de la Caja*", detallando:

> *"Robar las bases de datos, así como otra información de la Caja y de los asegurados eran los objetivos de los hackers, según confirmó hoy el Ministerio de Ciencia y Tecnología, que ha trabajado con esta institución afectada por el ataque.*
>
> *La violación de los sistemas informáticos, que se realizó en horas de la madrugada, fue considerada como "especialmente violenta y devastadora", tanto en los servidores físicos, como en la nube.*
>
> *La modalidad de vulneración de los sistemas informáticos utilizado por los delincuentes fue por medio de "ransomware", el cual, consiste en el robo de información y bases de datos, sin que se conozca el responsable del daño".*

Si bien esta Auditoría es consciente de las investigaciones en curso por la Administración en torno a las causas y consecuencias del evento de ciberataque a la CCSS, es importante considerar la necesidad de disponer de información concreta respecto del impacto que generó el mismo, y si existen datos personales comprometidos, o si hubo pérdida, destrucción, extravío, entre otras afectaciones, como consecuencia de la vulnerabilidad. Además, es vital la ejecución sistemática y organizada de acciones integrales en torno a medidas de seguridad (administrativas, físicas y lógicas), para garantizar la integridad y calidad de los datos personales que administra la institución.

En ese sentido, como es de conocimiento, a nivel nacional se dispone de la Ley No. 8968 referente a la Protección de la Persona Frente al Tratamiento de sus Datos Personales y su Reglamento, de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

En ese contexto, la Caja Costarricense de Seguro Social, como organismo público debe ajustarse a lo que establece la legislación y gestionar la información de conformidad con lo dispuesto en la normativa mencionada y su reglamento, esto tomando en consideración la relevancia de los datos que administra a nivel país en materia financiera, salud, pensiones y otros, por lo que deberá garantizar e implementar las medidas de seguridad correspondientes que estipula la reglamentación nacional en el tratamiento de los datos personales.

Al respecto, es importante recordar el rol de *"responsable"*[1], establecido en la ley como delegado de establecer y documentar procedimientos para el tratamiento de los datos personales (inclusión, conservación, modificación, bloqueo y supresión), así como el responsable[2] o encargado[3] de la base de datos el cual deberá vigilar por la aplicación de los principios de integridad, confidencialidad y disponibilidad de la información.

En el contexto de contratación o subcontratación de servicios, esta figura de "responsable" deberá comprobar que el *intermediario tecnológico* (la DTIC) *o proveedor de servicios* [4], implemente las medidas de seguridad necesarias que permitan garantizar la protección de los datos personales, y en términos generales, implantar los controles administrativos, físicos y lógicos para ese fin.

Así, es necesario se otorgue particular atención a lo establecido en la ley citada respecto a la participación del "responsable" en escenarios tales como; el de los ataques cibernéticos recientes, en donde se define un tiempo específico para informar -al titular- cualquier alteración en el tratamiento o almacenamiento de sus datos, a saber, destrucción, cifrado, robo, entre otros eventos similares, dentro de los que debe considerarse la vulnerabilidad materializada, lo anterior con el fin de que las autoridades institucionales procedan según corresponda dentro de la continuidad de servicios al usuario.

[1] "Toda persona física o jurídica, pública o privada, que administre o, gerencia o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, competente con arreglo a la Ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento les aplicarán".
[2] "Persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán".
[3] "Toda persona física o jurídica, entidad pública o privada, o cualquier otro organismo que da tratamiento a los datos personales por cuenta del responsable de la base de datos".
[4] "Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios".

Al respecto, el Reglamento a la Ley de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales, en el artículo 2, inciso “s”, establece:

> *s) Responsable: Toda persona física o jurídica, pública o privada, que administre o, gerencia o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, competente con arreglo a la Ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento les aplicarán.*

Ese mismo marco normativo, en el Capítulo IV, sobre el Tratamiento de los Datos Personales y las Medidas de Seguridad, señala:

> *“Artículo 29. Contratación o subcontratación de servicios. Se podrá contratar o subcontratar los servicios del intermediario tecnológico o proveedor de servicios, siempre y cuando no implique tratamiento de datos personales. El responsable deberá verificar que dicho intermediario o proveedor cumpla con las medidas de seguridad mínimas que garanticen la integridad y seguridad de los datos personales.*
>
> *Artículo 34. De las medidas de seguridad en el tratamiento de datos personales. El responsable, deberá establecer y mantener las medidas de seguridad administrativas, físicas y lógicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Reglamento. Se entenderá por medidas de seguridad el control o grupo de controles para proteger los datos personales.*
>
> *Artículo 38. Vulnerabilidad de seguridad. El responsable deberá informar al titular sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá cinco días hábiles a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.*
>
> *Dentro de este mismo plazo deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan.”*

Al respecto, este Órgano de Fiscalización y Control, mediante informe ATIC-83-2018, del 27 de julio 2018, en el estudio “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 Caja Costarricense de Seguro Social (CCSS)”, evidenció debilidades y oportunidades de mejora dentro de la atención de ese marco legal en la Institución recomendando el establecimiento de modelo de gestión integral orientado a garantizar ese cumplimiento normativo valorando:

- Definición de unidades institucionales a cargo del tema.
- Definición de roles y responsabilidades concretas según el ámbito de competencia.
- Mecanismos de coordinación entre los diferentes niveles de la organización.
- Elaboración y actualización de marcos normativos institucionales asociados a la Ley 8968 y su reglamento.
- Establecimiento de instancias y/o funcionarios encargados del monitoreo y seguimiento integral al cumplimiento de las acciones indicadas en la recomendación 3 del presente informe.

- Capacitación a nivel Institucional para los usuarios que participan en el tratamiento de datos personales, en torno a la aplicación de la Ley 8969 y su reglamento.
- Alineamiento con las iniciativas ejecutadas por la DTIC a través de la Licitación Abreviada No. 2016LA-000003-1150 “Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS”, lo anterior en lo que respecta a seguridad de la información en cumplimiento del marco normativo analizado en el presente informe.
- Revisión y actualización de los convenios firmados entre la CCSS e instituciones gubernamentales o empresas privadas para el acceso de información contenida en las bases de datos institucionales que contienen datos personales.

Así mismo, se señaló la necesidad de ejecutar las acciones correspondientes para elaborar un inventario institucional de todas las bases de datos que resguardan datos personales y efectuar las gestiones correspondientes para garantizar:

- Definición formal de los indicadores que deben considerarse en la clasificación de bases de datos según lo dispuesto en la Ley No. 8968.
- Categorización de las bases de datos que son internas y las que pertenecen al ámbito de aplicación de la Ley 8968, de acuerdo con lo establecido en atención del punto anterior. Al respecto, debe existir justificación suficiente, competente y pertinente sobre las bases de datos que resguardan datos personales y no forman parte del alcance del marco normativo analizado en el presente informe.
- Designación formal del responsable de cada base de datos, los encargados y el intermediario tecnológico, lo anterior en concordancia con las definiciones estipuladas en el reglamento a la Ley 8968.

Adicionalmente, se instruyó en su oportunidad, para que, a cada uno de los responsables en alineamiento al modelo de gestión establecido, ejecuten las acciones correspondientes, en aras de garantizar el cumplimiento de todas las funciones descritas en los artículos del Reglamento a la Ley 8968, a saber:

- Medio y forma de comunicación electrónica para facilitar a los titulares el ejercicio de sus derechos (artículo 16).
- b. Procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de datos personales (artículo 27).
- Mecanismos o procedimientos establecidos para comunicar a los encargados, las obligaciones en el tratamiento de bases de datos personales (artículo 31).
- Protocolos mínimos de actuación elaborados para la recolección, almacenamiento y el manejo de los datos personales. (artículo 32).
- Medidas de seguridad, administrativas, físicas y lógicas implementadas por el responsable para la protección de datos personales (artículo 34)

Finalmente, se recomendó en el informe que una vez identificadas las bases de datos ubicadas dentro del ámbito de aplicación de la Ley 8968, se instruyan a los responsables para ejecutar las gestiones correspondientes, a fin de inscribir dichos repositorios ante la Agencia de Protección de los Habitantes según los términos solicitados.

Por lo anterior, en el contexto de los eventos actuales de ciberseguridad, es necesario que al amparo de las acciones señaladas en el informe ATIC-83-2018 e implementadas por la Administración, active a la brevedad las medidas requeridas de acuerdo con las responsabilidades respectivas a cada Gerencia y Unidad institucional según los aplicativos afectados, lo anterior con el fin de garantizar el cumplimiento normativo, así como la protección de los datos personales administrados por la Caja Costarricense de Seguro Social de la población usuaria.

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

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.22 17:37:41 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OCHA/lbc

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva -1102
Máster Idannia Mata Serrano, subgerente, Dirección de Tecnologías de Información y Comunicaciones - 1150.
Auditoría