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

AS-AATIC-146-2022
14 de julio de 2022

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA – 2901

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA - 1103

Estimados señores:

ASUNTO: Oficio de Asesoría referente al procedimiento de registro y pago de incapacidades descrito en el oficio GF-0410-06-2022/GM-8071-2022 del 5 de julio del 2022.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo de esta Auditoria, para el período 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, este Órgano de Fiscalización a raíz del ataque cibernético sufrido por la institución el pasado 31 de mayo del 2022, emitió el oficio AS-AAFP-120-2022 el 30 de junio del 2022, dirigido a los titulares de la Gerencia Financiera, Dirección Financiera Contable, Dirección de Presupuesto, Dirección de Cobros y Direcciones Regionales de Sucursales Chorotega, Huetar Atlántica, Central, Brunca y Huetar Norte, en el cual se analizan las medidas contingentes para la gestión de ingresos y egresos.

En lo referente a procedimiento de pago de incapacidades, en el mencionado oficio esta Auditoría señaló la importancia de proteger información sensible de los asegurados realizando una asignación adecuada de los usuarios de los sistemas utilizados en esta tarea, además de velar por su modificación en el momento que sea restablecido el proceso normal.

Además, en función del restablecimiento del Sistema de Registro, Control y Pago de Incapacidades, se consideró necesario que se dirijan los esfuerzos institucionales al trámite de las boletas generadas mediante ese sistema y se abandonen los procedimientos manuales aplicados anteriormente, en virtud del riesgo de utilizar dos o más medios que afectarían tanto a la institución, como a quienes esperan el giro del subsidio.

En consonancia con lo anterior, el Dr. Randall Álvarez Juárez, gerente médico y el Lic. Gustavo Picado Chacón, gerente financiero procedieron a comunicar mediante el oficio GF-0410-06-2022/GM-8071-2022 del 5 de julio 2022, el restablecimiento del Sistema de Registro, Control y Pago de Incapacidades y los criterios técnicos de la imposibilidad de utilizar procedimiento alterno para procesamiento de incapacidades físicas mediante archivos de Excel, a los funcionarios que participan en las diversas etapas de este proceso, donde se indicó:

> "*En su momento, se dispuso el llenado de una plantilla de Excel, aprobada por los analistas de sistemas de información, como un medio para recopilar los datos de los talonarios y boletas adjudicadas a los profesionales médicos y odontólogos, así como de las incapacidades y licencias emitidas de manera física, que permitiera efectuar en forma emergente la carga de datos y el correspondiente pago.*"

Aunado a lo anterior, en el oficio mencionado los gerentes describen una serie de criterios relacionados con la utilización de la plantilla de Excel diseñada como medida contingente, entre los que se incluyen los de la Tesorería General de la Dirección Financiero Contable y la Subárea de Prestaciones en Dinero, donde se considera pertinente apegarse a lo indicado por la Subgerencia de Tecnologías de Información y Comunicaciones sobre la utilización del RCPI para el trámite de las boletas de incapacidad. Además de alertar sobre errores y omisiones en la información recibida afectando su integridad y exponiendo a la administración a errores.

Adicionalmente, instruyen a los establecimientos de salud a proceder con la inclusión de las incapacidades previamente remitidas en el archivo Excel, en virtud de evitar la concentración del proceso en las sucursales y la subárea de prestaciones en dinero, cuyos funcionarios además carecen del conocimiento necesario de la fase de registro y dado su número limitado podría alargar el proceso al menos 20 días adicionales.

En consonancia con lo anterior, dado que la digitación de la información contenida en las plantillas de Excel diseñadas como medida de contingencia ante la suspensión del funcionamiento del Sistema de Registro, Control y Pago de Incapacidades, será ejecutada por las unidades médicas generadoras del subsidio, eventualmente requerirá la habilitación de usuarios con perfiles de consulta y modificación de datos sensibles tales como: salarios, afectación a la salud, plazo de incapacidad, entre otros; es necesario informarles y capacitarlos respecto al marco de legalidad relacionado con la protección de dicha información, así como de los posibles efectos del no cumplimiento del marco jurídico atinente a este tema. Adicionalmente, la consideración de acometer esta tarea con la mayor calidad en los datos a incluir, dado que generan un egreso económico para la institución.

Además, considerando la estimación en el oficio gerencial mencionado con base a la cantidad de recurso humano disponible en las sucursales y en la subárea de prestaciones en dinero, la digitación de la información tomaría alrededor de 20 días, siendo este parámetro utilizado para instruir que dicho proceso sea asumido por las unidades médicas, requiere su atención a la brevedad posible y con la mayor celeridad a efectos de disminuir tanto el plazo como la afectación a los asegurados que esperan la materialización del pago del subsidio, en algunos casos desde el 1 de junio, ocasionando eventuales daños en la atención de sus necesidades básicas, siendo de gran preocupación aquellos casos en los cuales la incapacidad ha sido prolongada, así como las licencias por maternidad que se han otorgado en este lapso, sin disminuir la importancia de aquellas que responden a enfermedades de otras patologías.

Al respecto, el artículo 8 de la Ley General de Control Interno, establece:

> *"(…) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:*

a) *Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*

b) *Exigir confiabilidad y oportunidad de la información.*

c) *Garantizar eficiencia y eficacia de las operaciones."*

Respecto a la confidencialidad en el tratamiento de los datos la Ley de Protección de la Persona frente al tratamiento de sus datos personales, en su artículo 11 "Deber de Confidencialidad", establece:

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

Así mismo en el artículo 30 de la mencionada ley, se indica como falta grave:

> *"Serán consideradas faltas graves, para los efectos de esta ley:*
>
> *a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, con arreglo a las disposiciones de esta ley.*
>
> *b) Transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en el capítulo III de esta ley.*
>
> *c)Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información."*

Además, las Normas Técnicas para la Gestión y Control de las Tecnologías de Información promulgadas por el Ministerio de Ciencia, Innovación, Tecnologías y Telecomunicaciones, en su apartado XI "Seguridad y Ciberseguridad", establece:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
>
> *La Unidad de TI, basado en la política de seguridad de información / ciberseguridad, debe establecerlos mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.*

La institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, danos e interferencia a la información y los activos de información de la institución.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución."

De forma tal, dada la necesidad de satisfacer a la brevedad posible la necesidad de los asegurados de recibir el subsidio, eventualmente requerirá la creación de usuarios del sistema de Registro, Control y Pago de Incapacidades a efectos de asegurar su atención oportuna, los cuales deberán ser deshabilitados en el momento que cumplan su objetivo.

Además, de considerar la importancia de recordar a los funcionarios encargados de la inclusión de la información sus responsabilidades referentes al uso de los datos sensibles y personales de los asegurados, así como de velar por la calidad de los datos que sean incluidos con la finalidad de evitar errores en el proceso y eventuales afectaciones patrimoniales a la institución.

Debido a lo anterior, y con el fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a esa Administración Activa, para que realice una valoración de los aspectos señalados, y eventualmente se fortalezca las medidas de control interno sobre este particular.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.15 16:17:03 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AAM/lbc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General – 1100.
Auditoría.