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

AD-ATIC-0051-2023
28 de abril de 2023

Licenciado
Iván Guardia Rodríguez, director
DIRECCIÓN SISTEMA CENTRALIZADO DE RECAUDACIÓN - 1129

Estimado señor:

ASUNTO: Oficio de Advertencia referente a vulnerabilidad en Oficina Virtual CCSS.

La Auditoría Interna tuvo conocimiento del oficio SP-342-2034, del 16 de marzo 2023, suscrito por Rocío Aguilar M., Superintendente de Pensiones, en el que informó a la Dirección del Sistema Centralizado de Recaudación (SICERE), referente a denuncia recibida en la cual se hace de conocimiento una vulnerabilidad de la Oficina Virtual de la Caja Costarricense de Seguro Social (CCSS), la cual permite que los afiliados puedan ser trasladados de entidad autorizada, sin su consentimiento.

Una vez corroborado por ese órgano supervisor la existencia de la citada vulnerabilidad y dada la gravedad de la situación, así como para salvaguardar los intereses de los afiliados, dicha entidad instruyó a esa Dirección, ejecutar las siguientes acciones:

> *"1. Suspender de forma inmediata la posibilidad de realizar la libre transferencia por medio de la Oficina Virtual de la CCSS, utilizando la opción de autogestión, hasta que su representada corrija la situación detectada.*
> *2. Informar al público en general sobre esta suspensión.*
> *3. Realizar una investigación para determinar el origen de la vulnerabilidad, incluyendo posibles responsables, así como las medidas a adoptar. El resultado de esta investigación debe ser comunicado a esta Superintendencia para su análisis y posibles acciones de supervisión.*
> *4. Realizar las denuncias correspondientes ante el Ministerio Público, en caso de determinarse la eventual comisión de algún delito.*
> *5. Identificar los afiliados que fueron afectados por esta situación y remitir a esta Superintendencia el listado resultante, con el detalle de los datos personales que fueron modificados para realizar el traslado, la fecha y hora de ejecución, así como la entidad origen y destino involucradas".*

Dado lo anterior y de conformidad a las competencias establecidas en el artículo 22, inciso d) de la Ley General de Control Interno, a continuación, se procede a informar y advertir a la Administración Activa sobre los aspectos referentes a la situación supra indicada.

ACCIONES EJECUTADAS

De conformidad con lo anterior, esta Auditoría Interna evidenció las siguientes acciones para corregir los aspectos señalados:

1. El 16 de marzo de 2023, mediante oficio GF- DSCR- 0161-2023, el Lic. Iván Guardia Rodríguez, director del Sistema Centralizado de Recaudación, trasladó a la Licda. Susana Ureña Alvarado, jefe Área de Registro y Control de Aportaciones y al Lic. Alexander Angelini Mora, jefe de la Subárea de Servicios Financieros Administrativos de la Dirección de Tecnologías de Información y Comunicación, el oficio SP-342-2023, para su atención y conocimiento, en el que adicionalmente indicó:

   "…se agradece a la Subárea de Servicios Financieros Administrativos, la colaboración que pueda brindar para la atención de las mejoras y ajustes técnicos que sean necesarias, así como identificar los elementos de origen y generar la información que se requiera para el respectivo Informe.

   Por copia de la presente, se informa a la Licda. Lugo Mora, a fin de que brinde la colaboración correspondiente.

   Finalmente, se solicita mantener informado a este despacho sobre los avances en la atención de los puntos citados por la SUPEN

2. El 16 de marzo de 2023, con oficio GF- DSCR- 0164- 2023, el Lic. Guardia Rodríguez, director del Sistema Centralizado de Recaudación, informó a la Señora Rocío Aguilar M., Superintendente Superintendencia de Pensiones, se tomaron acciones inmediatas con el fin de realizar las revisiones exhaustivas y mejoras que se requieran, según se detallan:

   El 15 de marzo a las 4:30 pm, se deshabilitó en el perfil AFILIACION TRABAJADORES (OV) (perfil utilizado por los trabajadores), el menú por medio del cual se puede realizar la libre transferencia, tanto con el ingreso con usuario y contraseña como también con firma digital.

   El 16 de marzo a las 9:00 a.m. se deshabilitó la funcionalidad "Quiero Registrarme", por medio de la cual los usuarios realizan el autorregistro a la aplicación.

   Se está preparando el sistema para habilitar la libre transferencia delimitada al uso de firma digital para el perfil AFILIACION TRABAJADORES (OV), de modo que la opción esté disponible a más tardar el próximo martes 21 de marzo 2023.

   En cuanto al comunicado a los afiliados, a partir del 17 de marzo en horas de la mañana se dispondrá un mensaje informativo cuando el usuario ingresa a la Oficina Virtual CCSS…

   Cabe indicar que el servicio de libre transferencia continúa activo en el perfil AFILIACION CERTIFICADOR TRAMITADOR (OV), (perfil utilizado por la entidad origen y destino) por medio del cual las Operadoras de Pensiones pueden realizar la gestión con firma digital exclusivamente.

   Así mismo, se están generado acciones adicionales tendientes a identificar el origen de la situación detectada y las posibles libres transferencias aplicadas de forma improcedente, las cuales le serán informadas en cuanto sean concluidas.

   En cuanto a la petición recibida, mediante correo electrónico de fecha 16 de marzo 2023, suscrito por el Sr. Giovanni Fuentes y el cual se solicita le brindemos:

- *Cantidad de afiliados que realizaron la Libre transferencia por autogestión (TA) desde el 1 de julio 2022 al 15 de marzo 2023, se solicita facilitar la entidad origen y destino de cada transacción.*
- *Fecha estimada de atención del punto 5 del SP-342-2023.*

Sobre este particular, se le informa que procederemos a generar la información referida en el primer punto y estimamos poder remitirla el miércoles 22 de marzo".

3. El 17 de marzo de 2023, mediante oficio GF- DSCR- 0170- 2023, el Director del Sistema Centralizado de Recaudación, informó al M. Sc. Eithel Corea Baltodano, Subgerente a.i, de la Dirección de Tecnologías de Información y Comunicaciones, el funcionamiento según los requerimientos que en su momento fueron planteados para la funcionalidad "Quiero Registrarme" de la Oficina Virtual CCSS versus el comportamiento atípico identificado por la SUPEN, así como las acciones aplicadas para contrarrestar la vulnerabilidad, para lo cual le solicitó:

   "…colaboración a fin de que se realice una investigación que nos permita en principio, identificar la fecha desde la cual está en el ambiente productivo el fragmento de código que posibilitó el comportamiento inadecuado detectado en la funcionalidad "Quiero Registrarme" de Oficina Virtual CCSS explicado anteriormente y que generó un flujo que no responde a las reglas definidas en su momento para ese servicio.

   Dada la urgencia para atender este asunto, agradecemos nos puedan remitir dicha información en un plazo de cinco días hábiles a partir del recibo del presente oficio".

4. El 21 de marzo de 2023, con oficio GF-DSCR- 0177-2023, el Lic. Guardia Rodríguez informó a la Superintendencia de Pensiones sobre la funcionalidad de libre transferencia con firma digital Perfil AFILIACION TRABAJADORES (OV), lo siguiente:

   "…se le informa que el servicio fue habilitado el 20 de marzo del 2023 a las 5 p.m.
   En ese sentido, los afiliados podrán efectuar la libre transferencia con el perfil AFILIACION TRABAJADORES (OV), únicamente cuando el ingreso a la Oficina Virtual CCSS sea por medio del certificado de firma digital.

   De esta forma, en caso de que el afiliado ingrese utilizando el usuario y contraseña no se mostrará la opción para efectuar la libre transferencia.

   En virtud de lo anterior, se informa a su representada sobre las acciones realizadas por esta Dirección, para que adopten las medidas que considere oportunas y necesarias en cuanto a la divulgación a las entidades autorizadas

   Nos mantenemos trabajando en las demás acciones indicadas en el oficio DSCR- 0164-2023 y conforme se avance en ellas, le estaremos informando".

5. El 22 de marzo de 2023, mediante oficio GF-DSCR-0184-2023, el Lic. Guardia Rodríguez, remitió a la Licda. Rocío Aguilar Montoya, Superintendente de Pensiones, la información solicitada sobre libre transferencia tipo TA, indicando:

   "…de conformidad con lo solicitado, le informo que en archivo de Excel adjunto denominado: TA_julio 2022 al 15 marzo 2023.xlsx, se remite la cantidad afiliados que realizaron la Libre

transferencia con el perfil Afiliación Trabajadores (OV), para el periodo comprendido del 1 de julio 2022 al 15 de marzo 2023. Dicho archivo contiene los siguientes campos:

- *FEC_TRASLADO: Corresponde a la fecha de aplicación de la libre transferencia.*
- *TIP_FONDO: FCL o ROP según corresponde al fondo para el que se aplicó libre transferencia.*
- *ENTIDAD_ORIGEN: Entidad origen del traslado.*
- *ENTIDAD_DESTINO: Entidad destino del traslado.*
- *DIR_ IP: Dirección IP donde se registró el traslado".*

El 23 de marzo de 2023, con oficio GG-DTIC-1702-2023, el Máster Sergio Paz Morales, jefe del Área Ingeniería de Sistemas, informo al M. Sc. Eithel Corea Baltodano, Subgerente a.i, de la Dirección de Tecnologías de Información y Comunicaciones, lo siguiente:

"…se realizó la investigación solicitada; una vez identificado el origen del error, el personal procedió a verificar por medio del control de versiones del código fuente del Sistema Oficina Virtual (OV), "módulo de autoregistro", la fecha desde la cual se encuentra el fragmento de código indicado corresponde a la versión del Sistema implementada en octubre del 2017. Esta versión del Sistema OV, responde a la atención del requerimiento CUDS-R561 "Mejoras en diseño y navegabilidad para la interface de usuario de la Oficina Virtual del SICERE", así comunicado mediante oficio GG-DTIC-0003-2018 de fecha 02 de enero del 2018, del cual se sustrae y para lo que interesa, cito:

> *"La nueva versión de la Oficina Virtual quedo en producción el día 14 de octubre del 2017 y acta de aprobación de producción fue firmada el 05 de diciembre de 2017, luego de ajustar todos los temas pendientes…"*

Sin embargo, me permito aclarar que lo anterior no significa que la situación detectada por la SUPEN el pasado 15 de marzo del año en curso mediante una denuncia, se hubiera materializado desde octubre del 2017, ya que no se cuenta con reportes o incidentes concretos de comportamientos anómalos o atípicos en los procesos de autoregistro durante este tiempo".

El 28 de marzo de 2023, mediante oficio GF-DSCR-0210-2023, Lic. Iván Guardia Rodríguez, Director del Sistema Centralizado de Recaudación, señaló: *"…referente a las acciones para determinar el origen de la situación presentada, así como la determinación de los afiliados que fueron afectados, son acciones que se encuentran en curso de atención; por lo cual una vez ejecutadas las mismas se estará informando lo correspondiente".*

El 31 de marzo de 2023, con oficio SP-436-2023, la Señora Rocío Aguilar M., Superintendente de Pensiones, indicó al Lic. Iván Guardia Rodríguez, director del Sistema Centralizado de Recaudación, los siguientes aspectos:

Esta Superintendencia de Pensiones se refiere a los puntos 3 y 5 del oficio SP-342-2023 del 16 de marzo de 2023, en el cual se le informó sobre una vulnerabilidad de la Oficina Virtual de la Caja Costarricense de Seguro Social (CCSS), la cual permitía que los afiliados fueran trasladados de entidad autorizada, sin su consentimiento. Al respecto, es interés de esta Superintendencia conocer el avance de su representada en la atención de las acciones indicadas, así como las fechas en que se estima serán finalizadas.

Adicionalmente, como complemento de lo requerido en el punto tres, se solicita informar la fecha a partir de la cual se introdujo en la programación (software) de la plataforma de afiliación de la Oficina Virtual de la CCSS, el código identificado como "malicioso" (puerta trasera) que dio origen a la vulnerabilidad detectada.

Las Normas técnicas para la gestión y el control de las tecnologías de información y comunicaciones, versión 2.0., del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), señalan:

X. DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMA DE INFORMACIÓN

"La Unidad de TI debe aplicar prácticas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida.

La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones".

XI. SEGURIDAD Y CIBERSEGURIDAD

"La Institución debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La institución debe implementar medidas de control asociadas a la administración del riesgo de seguridad de la información y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información".

Es criterio de este Órgano de Control y Fiscalización, que la Dirección del Sistema Centralizado de Recaudación, carece de un plan que permita conocer el avance en la atención de las acciones propuestas para subsanar y/o fortalecer la vulnerabilidad informada por el órgano Superintendente, así como para comprobar el origen de la situación presentada, los responsables, el tiempo en la cual se introdujo la inconsistencia en la plataforma y los eventuales afectados por esa situación.

Al respecto, la falta de consentimiento en el traslado de usuarios de una operadora de pensiones a otra puede tener graves consecuencias económicas. Esto se debe a que las utilidades generadas por la antigüedad en la cartera de la operadora original pueden perderse en el proceso de cambio, además, podría afectar su pensión en el futuro, debido a que, con el paso del tiempo los rendimientos constituyen el principal componente del capital acumulado para su jubilación.

En ese sentido, la institución debe garantizar a los usuarios que los productos y servicios de TI, se generen de conformidad con los requerimientos de los interesados y con un enfoque de eficiencia y mejoramiento continuo; que respondan adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una continua valoración de riesgos; se debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales, y finalmente, el recurso humano tiene que conocer y estar comprometido con las regulaciones sobre la seguridad y confidencialidad, con el fin de reducir los peligros de error humano, robo, fraude o uso inadecuado de esos recursos.

En virtud de lo descrito, se informa y advierte al Director del Sistema Centralizado de Recaudación, para que, en cumplimiento de sus potestades y competencias, implemente de inmediato un cronograma de trabajo con las medidas de control pendientes o en proceso de ejecución, para subsanar la vulnerabilidad informada por la Superintendencia de Pensiones en la plataforma de afiliación de la Oficina Virtual de la CCSS, en el cual se brinde un detalle del avance en la atención de las labores propuestas, así como las fechas en que se estima serán finalizadas; de igual forma, ejecutar lo pertinente a efectos de determinar el origen de la situación presentada, sus responsables, y los afiliados que fueron afectados por esta situación, de manera que se cumpla con lo requerido por el órgano competente.

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 15 días, a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.04.28 10:41:39 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RAHM/OCHA/jfrc

C. Licenciado Luis Diego Calderón Villalobos, Gerente Financiero - 1103.
M. Sc. Eithel Corea Baltodano, Subgerente Dirección de Tecnologías de Información y Comunicaciones - 1150.
Auditoría

Referencia: ID-87635