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

AS-AAO-149-2022
15 de julio de 2022

Doctor,
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL -1100

Estimado señor:

ASUNTO:	**Oficio de asesoría referente a la afectación generada a los procesos sustantivos de la Dirección de Comunicación Organizacional debido al ataque cibernético en la CCSS.**

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, se informa sobre la importancia de fortalecer los procesos sustantivos asociados con la comunicación institucional, de manera que este proceso se mantenga de forma permanente entre la Institución y los usuarios internos y externos, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa Administración.

Los temas expuestos en el presente oficio encuentran fundamento en el análisis de la siguiente documentación suministrada por la Dirección de Comunicación Organizacional: DCO-501-2015 del 24 de octubre 2015, DCO-263-2016 del 17 de mayo 2016, DCO-419-016 del 26 de julio de 2016, DCO-020-2018 del 23 de enero 2018, DCO-464-2018 del 13 de noviembre 2018, DCO-0309-2021 del 24 de agosto 2021, GG-2704-2021 del 17 de agosto 2021. Asimismo, se llevó a cabo reunión el 27 de junio del 2022 con funcionarios de la Dirección de Comunicación Organizacional.

1. ANTECEDENTES

El pasado 31 de mayo del 2022, la Institución se vio afectada por un ataque cibernético, situación que conllevó a desactivar los sistemas informáticos de manera preventiva.

Según se indicó en el oficio AS-AATIC-113-2022 del 27 de junio de 2022, emitido por este Órgano de Fiscalización, tras cumplirse más de 20 días de ese incidente, la Institución restableció el funcionamiento de algunos sistemas de información, tal y como lo anuncia el medio de comunicación nacional “amprensa” en el titular “CCSS anuncia que su página web y plataforma de pagos ya fueron restablecidas” publicado el 21 de junio del 2022, citando:

> *“...Este martes la Caja Costarricense de Seguro Social, CCSS, anunció que la Presidencia Ejecutiva y la Gerencia General agradecían el trabajo realizado que permitió restablecer la página web de la Caja y la plataforma de SICERE.*
>
> *La plataforma de pagos de Sistema Centralizado de Recaudación, SICERE, permite a los patronos mensualmente presentar y facturar planillas.*
>
> *...La Caja ha anunciado que se encuentran trabajando arduamente en restablecer los sistemas pero que irán poco a poco...”*

2. ASPECTOS GENERALES

La Caja Costarricense de Seguro Social, es una de las instituciones públicas más complejas, la proyección de su imagen y el cumplimento de los objetivos establecidos, dependen en gran medida de una comunicación efectiva en todos los niveles, que permita lograr la aceptación de políticas, entender con claridad las leyes y reglamentos, fortalecer el flujo de información y promover la innovación para el desarrollo de la organización. Lo anterior, según lo establecido en el Manual de Organización de la Dirección de Comunicación Organizacional.

Corresponde a la Dirección de Comunicación Organizacional liderar el proceso de comunicación, su misión está orientada a desarrollar y mantener una comunicación dinámica, estratégica y permanente entre la Institución y los usuarios internos y externos, a fin de fortalecer la imagen institucional, la educación, la promoción de la salud, el fomento de estilos de vida saludables, el sentido de pertenencia y la cultura contributiva, en beneficio de la Seguridad Social.

En este sentido, la afectación sufrida por la Institución debido al ataque cibernético impactó en los objetivos propuestos en la Dirección de Comunicación Organizacional al verse limitado su sistema de comunicación, el cual, permitía mantener informados, tanto a usuarios internos, como externos en diversos temas institucionales.

Lo anterior, considerando que esta unidad administra la parte informativa del sitio web institucional, además, emite semanalmente comunicados de prensa (entre 3 y 5 diarios), y en virtud que la Institución tiene más de un millón cien mil seguidores en las diferentes redes sociales y que la página de la CCSS es de las más seguidas del país. Este proceso se convierte en un pilar relevante para generar una empatía con la población y una conexión constante con los asegurados. Como dato general, para el año 2021 la página de la CCSS durante el periodo comprendido entre el 01 de enero al 31 de diciembre 2021, y según reporte de Google Analytics, recibió un total de 28 040 222 (veintiocho millones cuarenta mil doscientos veintidós) vistas.

A continuación, se presenta el detalle de las actividades que se han visto afectadas a raíz del ataque cibernético en la Dirección de Comunicación Organizacional, asimismo, se citan las acciones contingenciales a las que se ha recurrido para mantener una comunicación interna y externa, en el tanto se reestablecen los servicios, y finalmente se exponen acciones realizadas con la finalidad de que se les dote de recurso humano para el fortalecimiento de sus procesos, según documentación analizada que contempla los periodos del 2015 al 2021.

3. SOBRE LA AFECTACIÓN GENERADA A LA COMUNICACIÓN INSTITUCIONAL CON USUARIOS INTERNOS Y EXTERNOS A NIVEL NACIONAL

Entre las primeras afectaciones que fueron identificadas por la Dirección de Comunicación Organizacional, se cita que, transcurrido el día dos después del ataque cibernético, los usuarios se sintieron directamente afectados en cuanto al pago de sus incapacidades, convirtiéndose éste en un tema sensible, situación que fue del conocimiento de las autoridades superiores. Además, se indicó que se logró percibir un alto volumen de preocupación de la población a raíz de este ataque cibernético, generando presión hacia la Institución debido a los servicios que se habían dejado de prestar de forma diferenciada, y el efecto en la ciudadanía al verse imposibilitada para tramitar citas por internet, retirar medicamentos, o reprogramar citas. Añaden los funcionarios de la Dirección de Comunicación Organizacional, que toda esa presión se reflejó en las redes sociales, y es consecuente con la problemática que la institución no ha podido resolver de forma integral.

Debido al hackeo el medio de comunicación oficial interno mediante correo electrónico se paralizó, a lo externo no se disponía de los accesos a la web institucional, ni de otros mecanismos de conexión. Por otra parte, se redujo la conectividad, lo que perjudicó al personal que se encontraba laborando en oficina, ya que debía atender conferencias de prensa, descargar imágenes, sonidos, videos, editar y realizar el procesamiento de la información, además, la publicidad que se encontraba activa se tuvo que suspender.

Una de las funciones sustantivas de la Dirección de Comunicación Organizacional establecida en su Manual de Organización, refiere a ejercer la rectoría en materia de comunicación institucional, con base en los requerimientos del nivel superior, los lineamientos y estrategias definidos, con el propósito de orientar el desarrollo de la gestión, además a esa Dirección, dentro de sus tareas le corresponde verificar que la información de interés institucional se difunda con oportunidad y calidad, conforme con los requerimientos de las autoridades superiores y la normativa vigente, con la finalidad de que la población y los funcionarios apoyen el desarrollo de la organización y se identifique con la ejecución de los programas institucionales.

Nótese entonces que al menos dos de esas funciones sustantivas, relacionadas con la rectoría y la oportunidad en la divulgación de la información, se vieron afectadas ante el evento de desconexión de los sistemas, generando esto una afectación generalizada en materia de comunicación.

4. SOBRE LAS ACCIONES CONTINGENCIALES

Producto del ataque cibernético y siendo que la Dirección de Comunicación Organizacional mantenía, tanto a lo interno, como a lo externo una divulgación de información, además, que estos canales de servían de enlace con otras plataformas en materia de promoción y publicidad, se establecieron una serie de acciones contingenciales entre las que se destacan; el restablecimiento de una versión simplificada de la web mediante la cual, la población lograra ingresar a la página institucional, visualizar mensajes, noticias, y tener información de lo acontecido en la Institución a raíz del ataque cibernético. Por otro lado, se han realizado envíos de comunicados de prensa a los medios de comunicación a través de grupos de WhatsApp y de Telegram. Se elaboraron listas de correo electrónico para enviar los comunicados de prensa a los medios de comunicación, a diputados, y a grupos de interés.

Además, los funcionarios de la dirección utilizan sus datos de internet para efectuar transmisiones en Facebook, descargar imágenes, sonidos y videos. Se debieron readecuar los mensajes, y dar paso a las campañas de comunicación orientadas a explicar a la población por medio de conferencias de prensa y redes sociales, lo que estaba sucediendo en la Institución, en lo que se está trabajando, a fin de afectar en lo menos posible la imagen pública de la CAJA.

Sobre este particular, la Auditoría Interna a través del oficio AS-ATIC-114-2022, de fecha 4 de julio de 2022, asesoró a las Gerencias sobre el uso de WhatsApp para el envío y recepción de información institucional, en los siguientes términos, relacionados con los riesgos de ciberseguridad de esa plataforma:

- *"...Al ser una plataforma abierta y de uso masivo, es posible trasmitir malware o efectuar actos de ingeniería social que permitan el robo de información sensible, infectar la plataforma tecnológica de la CCSS, secuestrar datos, entre otros.*
- *Posibilidad de nuevas vulnerabilidades, que podrían permitir acceder a datos confidenciales vía medios remotos.*
- *El cifrado punto a punto que ofrece WhatsApp, no necesariamente protege el acceso a datos de vulnerabilidades de tipo malware.*
- *No existe control de usuario sobre las copias de seguridad de información que realizan los dispositivos móviles, debido a que pueden respaldar en Cloud (en la Nube) datos confidenciales en cuentas de almacenamiento personal, lo que podría prestarse para fugas de información.*
- *WhatsApp hasta el momento no tiene la función de notificar cuando algún usuario realiza capturas de pantalla de los chats, lo que podría originar fugas de información...*

  ... De acuerdo con la información general y las observaciones indicadas anteriormente en torno al uso de la herramienta Whatsapp como medio de comunicación de información institucional, ya sea en el contexto de contingencia ante la interrupción de servicios tecnológicos producto del ciberataque, como en el desarrollo usual de las funciones, esta Auditoría considera necesario se defina en conjunto con las instancias correspondientes, una estrategia integral orientada a valorar los riesgos asociados al uso del Whatsapp, con el fin de normar y regular el uso del mismo por parte de los funcionarios de la CCSS en el contexto de la gestión institucional, tomando en cuenta los diferentes escenarios en los cuales se evidencia su utilización actualmente, y estando consientes de la transmisión y almacenamiento que realiza dicho aplicativo sobre imágenes, vídeos, audios, notas de voz, documentos, ubicaciones, contactos, llamadas y videollamadas, entre otros datos que podrían estar catalogados como confidenciales, sensibles y personales..."

Por su parte, las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, apartado "Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos", señalan:

> *"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*
>
> *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."*

La Caja Costarricense de Seguro Social constituye una de las instituciones públicas más importantes de este país al proporcionar servicios de salud y protección económica, social a los ciudadanos. En este sentido, es fundamental la proyección de su imagen pública y la comunicación que mantenga con los usuarios, tanto internos, como externos a nivel nacional.

Ante el evento sufrido por la Institución (ataque cibernético), son varias las lecciones aprendidas a considerar, siendo que quedó demostrado que los usuarios se sintieron directamente afectados al no recibir de forma habitual los servicios que brinda la Institución, ya sea en calidad de pacientes como trabajadores, pensionados y patronos, entre otros, sentir que se ha reflejado en las diferentes redes sociales que mantiene la Institución. Es claro que la Dirección de Comunicación Organización como ente rector en esta materia realizó acciones a fin de lograr reestablecer y mantener esa comunicación con los usuarios, a fin de reducir esa incertidumbre y preocupación que albergaba a la población nacional, por ejemplo, en temas críticos como lo es el pago de incapacidades, no obstante, se deben establecer estrategias a futuro que permitan de forma contingencial, garantizar de manera segura la comunicación interna y externa, con asegurados y funcionarios institucionales.

Debido a lo anterior, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a la Gerencia General, para que realice una valoración de los aspectos señalados, de manera que se fortalezcan las estrategias y acciones que se han establecido para lograr una comunicación dinámica, estratégica y permanente a los usuarios internos como externos a nivel nacional, a fin de que garantice la continuidad de las operaciones.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.15 17:23:45 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/ANP/MZS/MRPH/ghc

C. Licda. Xinia Fernández Delgado, directora, Dirección de Comunicación Organizacional - 1115
Auditoría