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

AS-AATIC-114-2022
4 de julio 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 TECNOLOGÍAS - 1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES – 9108

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

Estimados(a) señores(a):

ASUNTO:	**Oficio de Asesoría referente al uso de WhatsApp para el envío y recepción de información institucional.**

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 uso de WhatsApp para el envío y recepción de la información institucional como medio de comunicación contingente luego del ataque cibernético y la desconexión de los sistemas, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa Administración.

ANTECEDENTES

El 31 de mayo 2022, se registró en horas de la madrugada un ciberataque en contra de los servidores e infraestructura de telecomunicaciones de la CCSS, el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

De esa forma, 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".*

En primera instancia se detectaron 30 servidores infectados, no obstante, de conformidad con el informe brindado por el periódico digital "Delfino", el hackeo afectó más de 800 servidores. Al respecto, el artículo publicado el 1° de junio de 2022, indicó:

> *"La Caja indicó ayer que el ataque, perpetrado en horas de la madrugada, fue "excepcionalmente violento" y que por ello se procedió a apagar todos los sistemas críticos de la institución, particularmente unos que generan bastante afectación a la población, incluido el Expediente Digital Único en Salud (EDUS) y el Sistema Centralizado de Recaudación (SICERE) (…)*
>
> *La dimensión del ataque era mayor a lo que se me había indicado ayer cuando hablé del tema. Desafortunadamente, en realidad son 800 servidores afectados y tenemos 9000 terminales de usuario afectadas (computadores personales para cada funcionario).*
>
> *El presidente ejecutivo de la institución afirmó además que, "hasta donde sabemos", la información de los sistemas más críticos de la institución sí se pudo conservar, pues hay respaldo de estos hasta el pasado 30 de mayo, por lo que por ese lado damos la información que se habrá perdido de manera irrecuperable parece estar bastante controlada".*
>
> *Sin embargo, y esto tiene que ver con la naturaleza de cómo funciona este tipo de hackeo, la manera en que entraron los hackers dañó el acceso a los sistemas y eso es distinto a las bases de datos. Por ello reparar estos accesos a los sistemas toma bastante más días de lo que se indicó ayer, y no se ve posible restaurarlos esta semana", agregó Ramos (…)"*

Así mismo, también se solicitó a todos los establecimientos de salud mantener apagados los equipos de cómputo conectados a la red institucional, a fin de realizar el diagnóstico correspondiente de la afectación.

En ese sentido, esta Auditoría - mediante visitas realizadas a unidades médicas y sucursales y consultas efectuadas a funcionarios - tuvo conocimiento sobre el uso de la aplicación WhatsApp como medio de comunicación contingente para enviar y recibir información asociada con la atención de la emergencia, ejecución de labores y operatividad de los servicios, así como para la comunicación interna entre los empleados.

Lo anterior ante el impacto del ciberataque a los sistemas y servicios digitales tales como: el correo electrónico y la herramienta Microsoft Teams, esto debido a la aparente ausencia o desconocimiento de mecanismos de continuidad del negocio en ese sentido.

ASPECTOS GENERALES DE APLICACIÓN WHATSAPP

La aplicación Whatsapp es una herramienta de mensajería instantánea perteneciente a la compañía Facebook Inc., la cual es utilizada actualmente por más de 2000 millones de usuarios. La misma se brinda de forma gratuita, tal y como sucede con Facebook e Instagram, que también forma parte de las herramientas ofrecidas por dicha empresa.

En ese sentido, ningún producto de WhatsApp se licencia, es gratuito y bajo ese esquema no existe diferencia entre WhatsApp "Business" y WhatsApp personal, ya que lo que cambia es el tipo de cuenta en la versión "Business" que permite catalogarla como empresarial.

WhatsApp como aplicación dispone de las siguientes características de seguridad:

- Cifrado de extremo a extremo en todos los chats, por lo que todos los mensajes, llamadas, fotos, videos y demás multimedia están cifrados, y por tanto solo el emisor y el receptor pueden leer los mensajes. WhatsApp utiliza el modelo de encriptación de la aplicación de mensajería instantánea Signal (Open Whispers Systems).
- Función de bloqueo de huellas digitales para resguardo de los chats con datos biométricos.
- Tiene soporte para la autenticación de doble factor o autenticación en dos pasos (2FA), lo cual añade una segunda capa de protección a la contraseña que empleamos.

PROPIEDAD DE DATOS COMPARTIDOS MEDIANTE WHATSAPP

Si bien esta herramienta tiene cierto nivel de seguridad como se observó anteriormente, es necesario considerar que la empresa **Facebook Inc. como dueña de la misma puede hacer uso de los datos** recopilados mediante WhatsApp, Facebook e Instagram.

El objetivo de Facebook Inc. al obtener esta información es aprovecharla en conjunto con la obtenida de las otras aplicaciones para construir perfiles personalizados de los usuarios, con el fin de conocer sus intereses y ofrecer bienes y servicios para eventualmente obtener beneficios de la publicidad y comercialización.

Adicionalmente, ante la propiedad de uso de datos, Facebook tiene la potestad de cambiar los acuerdos de uso de información con el usuario en cualquier momento, lo cual podría materializar eventualmente un riesgo de privacidad en el que ni el funcionario que lo utilice, ni la Institución pueden intervenir.

RIESGOS DE CIBERSEGURIDAD

Si bien es de conocimiento el impacto y afectación a los sistemas de la organización a causa del ciberataque, es menester de este Órgano de Control y Fiscalización, recordar a la Administración Activa que también existen riesgos de tramitar información por medios que no están tipificados como oficiales y que debe ser conocidos por el personal de la institución, a saber:

- 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.

PRODUCTOS DE AUDITORÍA

La Auditoría Interna respecto al uso de WhatsApp, ha señalado que el mismo corresponde a un mecanismo de comunicación no oficial, detallando adicionalmente lo siguiente:

- En el informe ATIC-221-2017 del 30 de octubre 2017, se evidenció el reporte de incidencias relacionadas con el funcionamiento de los aplicativos SIAC-SIES Urgencias, por medio de WhatsApp, donde al respecto se encargó a la Gerencia Médica:

  "…en apego al marco normativo aplicable en materia de protección de datos, seguridad de la información y Política para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la CCSS, ejecutar las acciones correspondientes para eliminar dicha práctica en la gestión de incidencias, considerando los posibles riesgos de índole administrativo y legal a los que se exponen los usuarios que utilizan los aplicativos del Expediente Digital Único en Salud (EDUS-ARCA), como la Institución por el tratamiento inapropiado de los datos personales contenidos en las bases de datos de esa herramienta".

- La evaluación ATIC-203-2017 del 14 de diciembre 2017, señaló que los analistas de SIES en ocasiones atienden incidentes por aplicaciones móviles como WhatsApp, motivo por el cual se recomendó a la Gerencia Médica.

  "Conformar un equipo de trabajo encargado de definir una estrategia para analizar y reorganizar la gestión de incidencias de aplicaciones EDUS-ARCA en alineamiento a las decisiones que tome el Comité Estratégico y Gestor del Proyecto EDUS…".

- El informe ATIC-83-2018, del 27 de julio 2018, permitió identificar el uso de WhatsApp para reportar incidencias, consultas y otros temas relacionados con la gestión institucional, en el cual se encomendó a la Presidencia Ejecutiva.

  "Instruir a la Comisión conformada en atención de la recomendación uno del presente informe, defina un plan que establezca las acciones a ejecutar para mitigar los riesgos señalados por esta Auditoría en relación con las prácticas institucionales identificadas en el hallazgo 9 "Sobre prácticas de incumplimiento a la norma de protección de datos personales" del presente informe.

  Una vez definido el plan, deberán emitirse las directrices y mecanismos pertinentes, con el fin de evitar que las situaciones mencionadas se presenten en el futuro. Así mismo, debe considerarse la regulación en el establecimiento de las acciones que conforme derecho corresponda ante el incumplimiento de las normas y medidas definidas en torno a la protección de datos personales."

CONSIDERACIONES NORMATIVAS

Las Normas de Control Interno para el Sector Público, en el apartado 5.8 Control de sistemas de información, establece:

> *"El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter".*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, dentro de los procesos del marco de gestión de TI, en lo correspondiente al "Aseguramiento", establece:

> *"La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados".*

De igual forma, no se puede omitir el riesgo que genera el uso de mecanismo informales en el tratamiento de los datos personales. En ese sentido, la Ley No. 8968, en su Artículo 9, Categorías particulares de los datos, dispone:

> *"Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán se regirán por las siguientes disposiciones:*
>
> *1.- Datos sensibles*
> *Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros (…).".*

Así mismo, mediante oficio GM-AUDC-31997-2017, del 13 de noviembre 2017, la Dra. María Eugenia Villalta Bonilla, Gerente Médica en ese momento, emitió directrices indicando lo siguiente:

> *"…se insta a emitir un recordatorio a los funcionarios sobre las directrices que restringen el uso teléfonos celulares, radios localizadores, radios portátiles y otros en instalaciones de la CCSS, durante la jornada laboral y se instruya a la no utilización del WhatsApp como medio para reportar incidencias u otro relacionado con la prestación de servicios de salud. Aunado a ello, los informáticos de la institución no pueden brindar soporte técnico a ese tipo de herramientas, pues no existe un licenciamiento y soporte que pueda adquirir la CCSS", se evidencia que, a la fecha, WhatsApp continúa siendo utilizado con los fines antes expuestos.*

CONSIDERACIONES FINALES

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.

Lo anterior máxime considerando el panorama actual de vulnerabilidad que presenta nuestra Institución en torno a la protección de datos y ciberseguridad, así como la frecuente tendencia mundial por parte de atacantes informáticos de realizar este tipo de intrusiones, con afán de dañar la imagen de organizaciones y gobiernos, afectar la continuidad de los servicios y extorsionar instancias gubernamentales para obtener su propio beneficio a costa de la afectación a los ciudadanos.

En ese sentido, debe analizarse en ese contexto lo dispuesto en la "Ley 8968 de Protección de Datos de las Personas", en torno al acatamiento de lo dispuesto en el Artículo 5, inciso 2, donde se indica que "quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo",

Adicionalmente se requiere tomar en consideración lo dispuesto en otras normas relacionadas con esta temática, a saber, la Ley No. 8239 Derechos y Deberes de las Personas Usuarias de los Servicios de Salud Públicos y Privados, Ley No. 9234 Reguladora de la Investigación Biomédica, así como el Reglamento de Consentimiento Informado en la Práctica Asistencial de la CCSS; en particular referidas a datos -sensibles- de carácter personal relativos a la salud.

Como parte de la estrategia señalada, es importante considerar acciones intencionales en generar en el personal y en el asegurado, una cultura de conciencia y sensibilización con respecto a la seguridad de la información, los riesgos y amenazas existentes, lineamientos establecidos en la materia, métodos de ataque cibernético utilizados actualmente, importancia de la confidencialidad de los datos, medidas de control en el ámbito de acción respectivo y el debido cuidado en el uso de datos personales e institucionales a través de dispositivos de uso privado.

En forma complementaria, se plantean a continuación aspectos a valorar para instruir a los funcionarios sobre el uso de WhatsApp en el desarrollo de sus funciones, en dado caso se autorice luego de las valoraciones legales y técnicas que se realicen al respecto como parte de la estrategia mencionada anteriormente:

- Gestión y/o transferencia de información sensible, privada o confidencial, tanto interna, como de sus usuarios, en virtud de que no se pueden confirmar los niveles de seguridad del uso de esta aplicación en todos los dispositivos.
- Inhabilitación de la opción de descargas automáticas, ya que permite la descarga de cualquier archivo sin interacción con el usuario para verificar su confidencialidad o perjudicial para el dispositivo.
- Verificación y prueba de cifrado de extremo a extremo, para comprobar el cifrado de llamadas y mensajes enviados.
- Valoración de registro de datos personales en la tarjeta de información de contacto, esto con el fin de no exponer información de los trabajadores y mitigar los riesgos que esto conlleva.
- Garantizar que la aplicación esté actualizada a la última versión posible, además del sistema operativo del dispositivo.
- Instalar, utilizar y actualizar herramientas de protección, tales como: antivirus o de punto final que permitan analizar y bloquear las vulnerabilidades de spyware, malware y demás software malicioso.
- De igual forma, ante su uso o implementación en la institución, es fundamental se valore disponer de un instructivo con las normas que se deberán seguir e informar a los funcionarios (por ejemplo: las horas en que se realizan las comunicaciones, el contenido de los mensajes, el protocolo a la hora de enviar información sensible, entre otras cosas), dado que si no se gestiona correctamente puede dificultar la concentración, generar estrés y disminuir los niveles de productividad en el personal, igualmente, puede agobiar a los colaboradores en virtud de que suma otro flujo de información que deben revisar, lo que desdibuja la línea entre la vida laboral y privada.
- La organización deberá tener presente que WhatsApp es un formato de comunicación informal y que no sustituye a la comunicación institucional formal.

Finalmente, 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, en cumplimiento de sus potestades y competencias, valore lo indicado en el presente oficio y desarrolle a la brevedad las medidas que correspondan, con el fin de abordar los riesgos expuestos y otros relacionados a la comunicación de información institucional mediante medios personales y mecanismos no oficiales.

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 tres meses a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.04 14:18:19 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RHM/OCHA/lbc

C. Auditoría