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

AS-AATIC-169-2022
5 de agosto de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

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

Estimado(a) señor(a):

ASUNTO: Oficio de Asesoría sobre la gestión de ciberseguridad en el uso de dispositivos móviles.

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 la importancia de establecer acciones provisorias, con el propósito de soslayar la materialización de riesgos en materia de ciberseguridad generadas por el uso de dispositivos móviles (teléfonos inteligentes, computadoras portátiles, tabletas, entre otros).

1. GENERALIDADES

1.1. Antecedentes

Como ya es de conocimiento, la Caja Costarricense de Seguro Social (CCSS), fue obligada a desconectar todos sus sistemas informáticos y plataforma tecnológica de manera preventiva, producto del ataque cibernético que se materializó el 31 de mayo 2022. Dicha situación entre otras cosas evidenció la ausencia o desconocimiento de planes de continuidad del negocio e inclusive de las TIC[1], propiciando la utilización de dispositivos móviles como mecanismo de contingencia, particularmente de uso personal e inclusive propiedad de la CCSS, para enviar y recibir información asociada con la atención de la emergencia, ejecución de labores y operatividad de los servicios.

No obstante, la Auditoría Interna ha sido enfática con la Administración Activa, señalando en los oficios 53581 del 22 de agosto 2017 y AI-2328-19, del 19 de julio 2019, sobre los riesgos asociados con la seguridad informática y de la información por el uso de dispositivos móviles personales y propiedad de la misma Institución, para el trámite de la gestión institucional, en los cuales informó y advirtió respecto de los siguientes temas:

1. “Materialización de riesgos asociados a la seguridad informática y de la información debido a utilización de terminales no confiables, aplicaciones maliciosas, vulnerabilidades de infraestructura crítica e internet de las cosas (IoT por sus siglas en inglés), así como cualquier otra debilidad técnica que pueda ocasionar fuga y/o malversación de datos sensibles.

[1] Tecnologías de la información y las comunicaciones (TIC) es un término extensivo para la tecnología de la información (TI).

2. Promover el uso de las TIC, conforme a sus condiciones y recursos disponibles para optimizar y facilitar la prestación de sus servicios en cumplimiento de las tareas sustantivas que le han sido encomendadas, pero realizando un abordaje integral con respecto a la definición de un catálogo de los servicios tecnológicos disponibles para dispositivos móviles; de una política de uso, acuerdos de servicio y confidencialidad; establecimiento de los términos y condiciones para la utilización de los servicios de TIC por medio de aplicaciones para ese tipo de equipos por parte de usuarios externos, como asegurados y patronos; disponer de un marco regulatorio que establezca las directrices y mejores prácticas que a nivel institucional sean necesarias para promover la seguridad de la información e informática en los dispositivos móviles personales y tomar las acciones pertinentes para la mitigación de vulnerabilidades que puedan comprometer la continuidad en la prestación de los servicios tecnológicos.

   De lo contrario, se podría exponer a la Caja a posibles consecuencias de índole administrativo, civil o penal, según corresponda ante la ausencia de marco regulatorio, y mecanismos de control necesarios que minimicen riesgos asociados al posible uso inadecuado y/o fraudulento de la información contenida en las bases de datos institucionales por medio de los dispositivos mencionados.

3. En virtud de que estos equipos ofrecen la posibilidad de descargar, consultar y registrar información con la facilidad de transportarla a diferentes sitios que nuestra labor exige, tales como: capacitaciones, reuniones, y otras actividades inherentes a nuestras funciones, debe brindársele un uso apropiado a esta herramienta de trabajo.

4. Efectuar la socialización de las políticas, términos de uso y confidencialidad de la información que garanticen el cumplimiento de los lineamientos de seguridad, asignación, registro y uso de estos dispositivos".

Igualmente, mediante oficio AS-AATIC-114-2022 del 4 de julio de 2022, nuevamente se informó a la Administración Activa, sobre los eventuales riesgos a los que se expone la CCSS por el uso de WhatsApp[2] para enviar y recibir información institucional por medio de dispositivos móviles, según el siguiente detalle:

> *"…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".*

2. OBSERVACIONES

Dado lo anterior, en las siguientes observaciones se expone aspectos a considerar sobre el asunto de marras, las cuales podrán analizarse por la Administración Activa en la definición y/o implementación de estrategias en materia de ciberseguridad en el uso de dispositivos móviles:

[2] WhatsApp Messenger (o simplemente WhatsApp) es una aplicación de mensajería instantánea para teléfonos inteligentes (también cuenta con versiones para computadora, personal, business), propiedad de Meta.

- Es necesario que tanto los dispositivos institucionales, como los personales a los que se vaya a permitir el acceso a información institucional, cuenten con un antivirus confiable, el sistema operativo y aplicaciones debidamente actualizadas. Las principales razones de infección son por medio de troyanos al instalar software no seguro o legitimo; por medio de un phishing[3] al pulsar un vínculo malicioso recibido por correo electrónico, mensaje de texto o WhatsApp, y cuando se accede un enlace y este tiene una secuencia de comandos o guion (script) que va a detonar una vulnerabilidad de un software del dispositivo.

- Dentro de las vulnerabilidades que actualmente afectan los dispositivos móviles, se encuentra el malware llamado “MaliBot”, es software malicioso destinado al robo de contraseñas, datos bancarios, accede a mensajes de texto, registros de navegación, realiza capturas de pantalla y se propaga secuestrando las capacidades de SMS para enviar mensajes perversos a otros usuarios. El AlienBot, de la variedad de los troyanos, accede a información confidencial de la cuenta para adquirir el control del equipo, y finalmente, el Anubis -descubierto en el 2016- sigue siendo una amenaza activa dado la nuevas características y funcionalidades de troyano.

- Respecto a debilidades en la configuración de los dispositivos móviles, es bastante frecuente mantener activado el bluetooth, incluso cuando no es necesario, pero su principal problema no está en el gasto de la batería, sino por los riesgos a la privacidad que conlleva tener una señal abierta de forma permanente.

- Los dispositivos móviles propiedad de la institución contienen grandes volúmenes de información que se descarga o almacena por medio del acceso a correo electrónico, Microsotf Teams, servicios en la Nube, entre otros, siendo fundamental la protección de esos datos ante la perdida y/o robo. La organización deberá prestar atención a estos riesgos, a efectos de disponer de eficientes sistemas de administración de dispositivos móviles (MDM) según las necesidades y recursos disponibles, que permitan:

  - Supervisar el estado y la ubicación de cada dispositivo en tiempo real.
  - En caso de perder o extraviar un dispositivo, se pueda cambiar la contraseña y bloquear, incluso si no está conectado a Internet.
  - Si no se puede recuperar, se logre borrar de forma remota los datos del dispositivo, incluidos los almacenados en memoria o tarjeta SD.
  - Instalar directamente las aplicaciones que se requieran en el dispositivo individual o por grupos.
  - Auditar la actividad del usuario, llevando un control de los registros de llamadas y las aplicaciones instaladas.
  - Bloquear movimientos no seguros que puedan generar los funcionarios por medio del dispositivo.

- Otros aspectos para considerar por la Administración Activa para controlar y salvaguardar la información contenida por el uso dispositivos móviles personales o propiedad de organización, se fundamentan en el informe de buenas prácticas publicado por el Centro Nacional Criptográfico de España en mayo 2021, denominado “Dispositivos móviles”, donde se describe:

  - El sistema operativo del dispositivo móvil debe estar siempre actualizado.
  - Se recomienda no otorgar permisos innecesarios o excesivos a las apps.
  - Deshabilitar todos los interfaces de comunicaciones inalámbricas del dispositivo si no se utilizan.
  - No conectar el dispositivo móvil a redes Wi-Fi públicas abiertas.
  - Se deben realizar copias de seguridad (backups) periódicas.
  - Se debe hacer uso de las capacidades nativas de cifrado del dispositivo móvil.
  - No instalar ninguna aplicación móvil (app) que no provenga de una fuente de
  - confianza,
  - El dispositivo móvil debe estar protegido mediante un código de acceso robusto.

[3] El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta.

2.1. Seguridad en dispositivos móviles: principales amenazas

Si bien es cierto, desde antes del ciberataque la Institución ha venido promoviendo la prestación de servicios a través del aprovechamiento de las Tecnologías de Información y Comunicaciones, y en específico mediante el uso de dispositivos móviles, es preciso incrementar los mecanismos de seguridad y monitoreo garantes de la máxima protección de los datos. Para tales efectos, es posible la conexión a la Red Privada Virtual (Virtual Private Network VPN) o soluciones de virtualización que regulen el acceso al correo electrónico, aplicaciones institucionales, navegación web, así como los otros servicios albergados en la Nube.

A pesar de las ventajas que ofrece el uso y aprovechamiento de esos dispositivos, existen peligros asociados a la exposición de ataques por parte de los ciberdelincuentes, por cuanto todo equipo móvil conectado a internet podría eventualmente no disponer de elementos para generar un acceso seguro a las herramientas de trabajo mencionadas o incluso a los sistemas automatizados institucionales. Los creadores de algoritmos maliciosos están aprovechando las vulnerabilidades de seguridad o cualquier otra debilidad técnica que pueda ocasionar fuga y/o malversación de datos sensibles.

Entre las principales amenazas que podrían afectar la seguridad móvil, se encuentran:

- **Ataques de malware**, entre sus principales objetivos está el robo de credenciales y la recopilación de datos, tales como historial de llamadas, libreta de direcciones, registros de navegación web, posicionamiento, mensajes de texto, la cual extraen utilizando publicidad engañosa o falsa.

- **Ataques de Phishing**, son correos electrónicos (aunque pueden utilizar cualquier otro medio de mensajería) en los que se suplanta la identidad de una persona o entidad de confianza de la víctima, para hacer pulsar un enlace, donde en realidad se encuentra un software malicioso destinado a infectar o vulnerar el dispositivo.

- **Ransomware móvil**, en este caso son tácticas de ingeniería social con las que se engaña al usuario para descargar contenido malicioso, como aplicaciones falsas de tiendas de terceros, actualizaciones del sistema o de software infectado, o incluso para ingresar a direcciones indebidas por medio correo electrónico, mensaje de texto, etc., su objetivo es secuestrar o cifrar los archivos e información a cambio de un rescate para recuperarlos, normalmente se requiere en dólares y en un plazo determinado.

- **Man in the middle o ataque de intermediario**, consiste en obtener información sensible mediante la instalación de puntos de acceso a internet, en lugares públicos o redes inalámbricas sin restricción. Así, cuando los usuarios se conectan, dan acceso a los atacantes de forma involuntaria a sus dispositivos.

- **Alteraciones del sistema operativo**, alterar el sistema operativo del dispositivo móvil implica riesgos, se podrían deshabilitar las restricciones de seguridad que posee por defecto el equipo.

- **Fugas de información**, esta amenaza de seguridad sucede cuando una aplicación móvil, que teóricamente es legítima, en realidad captura datos nuestros, y los transmite a terceros.

- **Spyware**, es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

- **Criptografía quebrada**, ocurre cuando los desarrolladores de aplicaciones utilizan algoritmos de cifrado débiles o cifrado seguro sin una implementación adecuada. En el primer caso, los desarrolladores utilizan algoritmos previamente diseñados (para acelerar el proceso de desarrollo de aplicaciones), pero estos poseen vulnerabilidades ya conocidas por los ciberdelincuentes, por ende, el resultado es el descifrar las contraseñas y obtener acceso fácilmente. En el segundo, utilizan algoritmos altamente seguros, pero dejan abiertas otras “puertas traseras” que limitan su eficacia.

- **Gestión inadecuada de sesiones**, con el fin de facilitar el acceso a transacciones en dispositivos móviles, numerosas aplicaciones usan "tokens", que permiten a los usuarios ejecutar varias acciones sin necesidad de volver a autenticar su identidad. De manera semejante a las contraseñas, estos son generados por las aplicaciones como una manera de identificar los dispositivos. Las aplicaciones seguras generan nuevos tokens con cada intento de acceso o "sesión", y estos deben permanecer confidenciales.

Según Kaspersky Security Network[4] (compañía internacional dedicada a la seguridad informática), en el primer trimestre de 2022, se neutralizaron 6 463 414 ataques lanzados mediante software malicioso, publicitario o no deseado para dispositivos móviles. Los programas RiskTool[5], de la variedad de los malware, representó la mayor parte de todas las amenazas detectadas con el 48,75%. Asimismo, se detectaron 516 617 paquetes de instalación maliciosos entre troyanos bancarios y ransomware.

De conformidad con lo anterior y al crecimiento inevitable en el uso de equipos móviles, tanto personales, como los proveídos por la Institución (método llamado "bring your own device", BYOD por sus siglas), hace pensar que la seguridad debe ser cada vez más importante para garantizar la protección de los datos, siendo necesario se valoraren alternativas o métodos de movilidad institucional con el fin de asegurar, monitorear y administrar los riesgos que se puedan derivar de su utilización en la CCSS.

3. CONSIDERACIONES FINALES

En razón la relevancia de la información que administra la Caja Costarricense del Seguro Social a nivel país en materia financiera, salud, pensiones y otros, así como el aumento en el uso de dispositivos móviles para acceder o gestionar datos institucionales, es primordial contemplar los escenarios utilizados y se valore analizar el modelo de movilidad y seguridad utilizado actualmente por la Institución.

Por lo anterior y en el contexto de los eventos actuales de ciberseguridad, es necesario que al amparo de lo descrito en el presente documento y de las acciones señaladas en los oficios 53581-2017 y AI-2328-2019 e implementadas por la Administración, se active a la brevedad posible el marco regulatorio y mecanismos de control concretos que minimicen los riesgos asociados al posible uso y almacenamiento inadecuado y/o fraudulento de la información contenida en las bases de datos, correo electrónico o aplicaciones SaaS (Software como servicio) institucionales, accedidos por medio de los dispositivos mencionados, tanto personales como proveídos por la institución. Por ello, cualquier estrategia de movilidad debería incluir la solución técnica necesaria para dotar de independencia del dispositivo en caso de problemas, como un robo, extravío, infección por virus u otro tipo de circunstancia.

Sobre los equipos móviles aprovisionados por la Caja, es responsabilidad de la Administración Activa establecer las medidas correspondientes para garantizar la protección y conservación del patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal, como uno de los objetivos de control interno, de manera que su manejo, custodia y cuidado se encuentren acorde con las directrices institucionales y de los fabricantes en cuanto a seguridad, almacenamiento y limpieza.

Otro elemento por considerar en este escenario es la concientización y sensibilización del personal, un aspecto importante de seguridad para evitar ser vulnerable en el uso de dispositivos móviles, personales o colectivos, de manera que contribuya a la adopción de las políticas y estrategias de seguridad establecidas para el acceso a los datos y recursos de la organización. En caso de utilizar el dispositivo propio, se debe sensibilizar en aspectos tales como; el uso de contraseñas complejas de bloqueo/desbloqueo de sus equipos, realizar respaldos, uso de antivirus para el análisis de datos y aplicaciones, configurar opciones de bloqueo y/o borrado de datos del dispositivo en caso de pérdida o robo, entre otras buenas prácticas relacionadas con la ciberseguridad en esos equipos.

4 Evolución de las ciberamenazas en el primer trimestre de 2022. Estadísticas sobre amenazas móviles | Securelist.
5 RiskTool. Los programas de esta categoría poseen varias funciones (ocultar archivos en el sistema, ocultar ventanas que ejecutan aplicaciones, terminar procesos activos, etc.).

En ese sentido, las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "Seguridad y Ciberseguridad", lo siguiente:

> *"XI. SEGURIDAD Y CIBERSEGURIDAD*
>
> *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 establecer los 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, daños 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.*
>
> *La Unidad de TI 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 Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales".*

En cuanto a la gestión de riesgos tecnológicos, ese mismo marco normativo, en el numeral IV, dispone:

> *"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.*
>
> *La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución".*

Por su parte, las Normas de Control Interno para el Sector Público, señalan en el inciso 5.7.4 “Seguridad” lo siguiente:

> *“Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran”.*

Antes lo expuesto, es preciso se realice una valoración de los riesgos asociados a la gestión de ciberseguridad en el uso de dispositivos móviles en la Caja Costarricense de Seguir Social, a efectos de adoptar acciones que permitan no solo la continuidad de los servicios prestados sino también la protección, eficiencia y eficacia en la administración de los recursos institucionales.

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: 2022.08.08 11:21:46 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/OCHA/lbc

C. Auditoría