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

**AS-AATIC-138-2022**
11 de julio de 2022

Licenciada
Odilíe Arias Jiménez, directora
**DIRECCIÓN DE INSPECCIÓN -1128**

Estimada señora:

**ASUNTO: Oficio de Asesoría referente al uso de servicio de internet (MIFI) en la Dirección de Inspección como contingencia al ataque cibernético sufrido el 31 de mayo de 2022.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo del Área de Tecnologías de Información y Comunicaciones 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 diversos aspectos vinculados con la utilización del servicio de internet adquirido por personal de la Dirección de Inspección para la continuidad de las actividades sustantivas a cargo de varias áreas, lo anterior debido al ataque cibernético efectuado el pasado 31 de mayo de 2022 contra la Caja Costarricense de Seguro Social que ocasionó la desconexión de los servicios brindados a través de la Plataforma Tecnológica.

## Antecedentes

### Ataques cibernéticos a la Caja Costarricense de Seguro Social

El 21 de abril del 2022, la Caja Costarricense de Seguro Social recibió un ataque cibernético dirigido al Portal de Recursos Humanos, lo cual ocasionó que se deshabilitara el acceso a esa plataforma tecnológica durante 15 días aproximadamente, con el objetivo de limitar verificar si se logró el ingreso por parte de los atacantes o si hubo extracción de información sensible.

Posteriormente, el 31 de mayo de 2022, se detectó otro ciberataque, obligando a la Institución a deshabilitar la Infraestructura Tecnológica que soporta los diversos sistemas de informáticos, bases de datos y servicio de internet utilizados para la prestación de servicios a los usuarios en el territorio nacional.

El 1 de junio de 2022, a través de conferencia de prensa a medios nacionales, el Dr. Álvaro Ramos Chaves, presidente ejecutivo de la Institución, indicó lo siguiente:

> *"La Manera en la que entraron los hackers dañó la forma en la que los usuarios pueden acceder a los sistemas y reparar estos accesos toma bastante más días de lo que se indicó inicialmente. Ya sí les podría adelantar que no se ve posible restaurarlos esta semana, preferiría no adelantar cuánto más, pero esta semana no va a hacer"*

El 2 de junio de 2022, mediante oficio GA-CAED-0260-2022, el Dr. Mario Vílchez Madrigal, director a.i. del Centro de Atención de Emergencias y Desastres, remitió a los Gerentes, Directores de Sede, Directores de Red Integrada de Prestación de Servicios de Salud, Directores Regionales de Sucursales Financieras, Directores Generales y Administrativos Financieros de Hospitales y Directores y Administradores de Áreas de Salud, lo siguiente:

> *"Procede a Validar el Estado de Emergencia Institucional, debido a los ciberataques sufridos por la Caja Costarricense de Seguro Social el 31 de mayo del 2022. De manera que, se solicita a todas las instancias aplicar las medidas necesarias para la atención de esta emergencia. Se instruye a mantener en operación los Centros Coordinadores de Operaciones Central, Regionales y Locales y a aplicar los mecanismos de excepción requeridos para la continuidad de los servicios. La Dirección de Presupuesto y el CAED informarán el procedimiento excepcional que se utilizará mientras los sistemas institucionales de TI sigan desconectados, mediante el cual se aplicará el Procedimiento para la gestión de la Reserva de Contingencia del Seguro de Salud (de la Caja Costarricense de Seguro Social),"*

## Dirección de Inspección

La Dirección de Inspección es una unidad adscrita a la Gerencia Financiera y tiene como objetivo fortalecer las acciones de cobertura contributiva y disminución de la evasión, por medio del aseguramiento de los trabajadores asalariados, la fiscalización de los patronos y los trabajadores independientes, así como el desarrollo de la asesoría y la capacitación a las unidades del nivel central y desconcentrado

Además, esa unidad se encuentra estructurada internamente con 4 áreas y 11 subáreas como se muestra en la siguiente tabla

**Tabla No. 1**
**Áreas y Subáreas de la Dirección de Inspección**

| | Área | Subárea |
|---|---|---|
| **Dirección de Inspección** | Aseguramiento y Fiscalización Patronal de Servicios | • Servicio de Transporte<br>• Servicios Financieros<br>• Servicios Diversos<br>• Estudios Especiales |
| | Aseguramiento y Fiscalización Patronal de Industria y Comercio | • Industria<br>• Comercio<br>• Construcción<br>• Estudios Especiales |
| | Gestión Técnica | • Investigación<br>• Plataforma de Servicios |
| | Control Contributivo | • Administración y Control de Convenios |

**Fuente:** Elaboración propia, julio 2022.

## Mecanismos de contingencia implementados por la Dirección de Inspección

El 2 de junio de 2022, mediante oficio GFDI-0005-06-2022, la Licda. Odilíe Arias Jiménez, Directora de Inspección, remitió a las jefaturas de área adscritas a esa dependencia, las medidas transitorias y excepcionales como parte de la contingencia en la atención de las siguientes solicitudes:

- Afiliación de Trabajadores Independientes (TI), Asegurados Voluntarios (AV) y Asegurado Migrantes en plataformas.
- Recepción de solicitudes de estudio en plataformas
- Atención de las solicitudes por parte de jefaturas
- Atención por parte del Inspector

**Observaciones**

Como se ha expuesto en el presente oficio, el pasado 31 de mayo, la Institución sufrió un ataque cibernético que ocasionó la suspensión de los servicios brindados a través de sistemas informáticos como el Expediente Digital Único en Salud, Sistema Centralizado de Recaudación (SICERE), Registro, Control y Pago de Incapacidades (RCPI), Sistema Integrado de Gestión de Personas (SIPE), así como el acceso a Intranet e internet, entre otros.

Así las cosas, esta Auditoría en sesión de trabajo realizada con personal de la Dirección de Inspección el 21 de junio del presente año, tuvo conocimiento sobre la adquisición de servicio de internet mediante enrutadores inalámbricos conocidos como MIFI, con recursos propios de varias jefaturas de esa dependencia dentro de las iniciativas para brindarle continuidad a los procesos sustantivos a cargo ante la desconexión de la Plataforma Tecnológica.

Por lo tanto, teniendo en consideración la iniciativa desarrollada por varios funcionarios de esa Dirección, los ataques cibernéticos dirigidos hacía la Caja Costarricense de Seguro Social meses atrás y la normativa vigente aplicable en temas de telecomunicaciones, seguridad de la información y ciberseguridad, este Órgano de Fiscalización y Control, emite las siguientes observaciones con el objetivo de que sean valoradas y analizadas por la administración activa entre las labores de control interno implementadas mientras se restablecen los servicios brindados por la Institución:

- Los dispositivos inalámbricos vienen comúnmente configurados de fábrica con usuario y contraseña genéricas como por ejemplo ADMIN, 1234567, 1234, 4321, 0000 y/o 9999, aspecto conocido por los cibercriminales, quienes ejecutan ataques tratando de averiguar las credenciales de seguridad para lograr infiltrarse en la red y sustraer los datos gestionados por el negocio.

  En virtud de lo anterior, resulta relevante verificar que la clave de acceso de los aparatos de marras sea modificada, en caso de tener claves genéricas asignadas, se debe realizar su modificación teniendo en consideración las buenas prácticas para la definición de contraseñas relacionadas con la longitud recomendada de al menos 8 caracteres, la inclusión de letras mayúsculas y minúsculas, numerales y signos especiales.

- La contraseña seleccionada para limitar el acceso a los enrutadores debe ser única para cada componente tecnológico y confidencial, por lo cual no es recomendable la reutilización de claves y de requerirse su resguardo físicamente, debe ser en un lugar donde no pueda ser accedida por personas ajenas a la unidad. Además, resulta oportuno que la administración valore el establecimiento de procedimientos para el cambio de credenciales de forma periódica mientras se restablecen los servicios institucionales y se suspende su utilización.

- En caso de que los dispositivos inalámbricos adquiridos sean utilizados para brindar acceso a internet a equipos institucionales como computadoras y tablets en oficinas de la CCSS, es importante que sean considerados al menos los siguientes aspectos:

- Solicitud de aval del ente técnico a cargo de las tecnologías de información y comunicación, lo anterior con el objetivo de que se analicen posibles riesgos de ciberseguridad asociados al uso de los dispositivos de marras para acceder a internet.
- Autorización de los niveles jerárquicos superiores para su uso en instalaciones CCSS.
- Análisis de los equipos que se van a conectar a los enrutadores en aras de detectar oportunamente posibles vulnerabilidades de ciberseguridad que pongan en riesgo la información gestionada y los equipos de cómputo utilizados.
- Valoración de riesgos vinculados con la ausencia de protección por parte de software y hardware institucional especializado en protección, monitoreo y detección de ataques cibernéticos.
- Respaldo documental vinculado con la figura bajo la cual se suministran los dispositivos (adquisición, préstamo, donación).

**Consideraciones normativas**

La Ley General de Control Interno No.8292, en el artículo No. 8 — Concepto de sistema de control interno, establece lo siguiente:

> *"**Artículo 8º—Concepto de sistema de control interno***
>
> *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.*
>
> *d) Cumplir con el ordenamiento jurídico y técnico."*

10 —Responsabilidad por el sistema de control interno, establece lo siguiente:

> *"**Artículo 8 Artículo 10.—Responsabilidad por el sistema de control interno.***
>
> *Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado VIII. Contratación y adquisición de bienes y servicios tecnológicos, establece lo siguiente:

*"**VIII. Contratación y Adquisiciones de Bienes y Servicios Tecnológicos***

*La institución debe disponer de prácticas formales para establecer los requerimientos de contratación y adquisición de bienes, consultorías y servicios a proveedores externos, cuyo giro de negocio sea orientado al ámbito tecnológico, de forma tal que apoye el desarrollo de iniciativas y mejoras de la infraestructura tecnológica, sistemas de información, seguridad de la información, ciberseguridad y otros relacionados de acuerdo con las necesidades y oportunidades visualizadas al nivel institucional. El modelo debe permitir establecer objetivamente al nivel operativo, técnico, legal y tecnológico entre otros, los términos de referencia, los parámetros de valoración del perfil del proveedor y su oferta para realizar la selección adecuada."*

Esas mismas Normas, en los apartados X. Desarrollo, implementación y Mantenimiento de Sistemas de Información y XI. Seguridad y ciberseguridad y XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, señala:

*"**X. DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS 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 aplicar las prácticas de aseguramiento del cumplimiento contractual y las prácticas de calidad asociadas para los casos en utilice soluciones desarrolladas y/o implementadas por proveedores externos.*

*"**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 (…).*

*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 (…)"*

El Modelo de Organización de los Centros de Gestión Informática, en el apartado *"Gestión Técnica"*, establece las siguientes funciones:

*"Elaborar juntamente con los usuarios los términos de referencia para la adquisición y contratación de hardware, el desarrollo de sistemas de información y las aplicaciones, con base en la normativa y el manual de estándares vigente, con el fin de promover la comunicación y la integración de los recursos informáticos*

*Planificar la adquisición de software y hardware, de acuerdo con las necesidades de la organización, el presupuesto asignado, las estrategias, las políticas y la normativa de contratación administrativa vigente, con el fin de lograr la confiabilidad, la calidad de la información y la prestación óptima de los servicios".*

Teniendo en consideración que el MIFI cuenta con un chip de telefonía móvil, el Reglamento para la asignación, uso y control de líneas y aparato telefonía móvil, señala en los artículos No. 3 y No. 4, lo siguiente:

*"Autorización*
*Artículo 3.*

*La asignación de la telefonía móvil (línea, aparato y accesorios) se realizará a los funcionarios de la Institución señalados en el artículo 9° del presente Reglamento.*

*Para los empleados que califiquen en el numeral d) y e) del artículo 9°, se requerirá de un estudio técnico, por parte de la Subgerencia de Tecnologías de Información y Comunicaciones, y su aprobación será potestad de la Gerencia respectiva. Este acto se otorgará de forma excepcional y restrictiva, siempre que exista una necesidad comprobada y manifiesta de que el funcionario por sus responsabilidades debe mantener un contacto constante y exclusivo con el área de trabajo*

*Artículo 4.*

*El estudio técnico mencionado anteriormente deberá considerar la naturaleza estratégica de las funciones que desarrolla el funcionario y la necesidad de una comunicación oportuna, que permita la resolución de problemas y la toma efectiva de las decisiones para favorecer la excelencia del servicio a los usuarios internos y externos.*

*Estos estudios deberán someterse a la aprobación de la Gerencia respectiva y demostrar que se dispone del contenido presupuestario en las partidas de "Equipo de Comunicación" y "Gastos de Teléfono".*

El Protocolo DSS02-PT-097 *"Enlaces inalámbricos móvil"*, establece las siguientes acciones a seguir para la solicitud de de enlaces inalámbricos móviles:

*"Paso No.1*

*El usuario debe de proporcionar la información completa a Nivel 1 (Mesa Servicios TIC): Nivel 1:*

- *Cantidad de dispositivos*
- *Justificación de la solicitud*
- *Unidad Ejecutora que asumirá el gasto de los dispositivos.*
- *Nombre usuario a quien se asignará el dispositivo*
- *Firma de la jefatura, administrador o director.*
- *Correo electrónico y número telefónico del contacto*

*Si la información no está completa, Nivel 1 indicará al usuario que complete la información solicitada. Fin de protocolo*

*Una vez facilitada dicha información Nivel 1 escala el caso a Nivel 2 (Soporte TIC Comunicaciones). Continua con paso 2.*

*Paso No.2*

*Nivel 2 (Soporte TIC Comunicaciones):*

- *Procede a la configuración del dispositivo y posterior entrega de los dispositivos solicitados.*
- *Informará del estado del caso a Nivel 1 (Mesa Servicios TIC)*

*Continua con paso 3.*

*Paso No.3*

*Nivel 1 (Mesa de Servicios TIC) validará con el usuario los resultados de la petición según la información proporcionada y procederá con el cierre respectivo."*

**CONSIDERACIONES FINALES**

La Dirección de Inspección de la CCSS tiene como misión ampliar la cobertura contributiva y el control de la evasión en su jurisdicción administrativa, lo anterior a través de la implementación de estrategias para el empadronamiento de patronos y el aseguramiento de los trabajadores.

Sin embargo, ante la desconexión de la Plataforma Tecnológica, debido a los ataques cibernéticos contra la Institución durante este año que limitaron el suministro de internet y acceso a diversos aplicativos informáticos institucionales, esa Dirección implementó mecanismos de contingencia para la ejecución de las actividades sustantivas vinculadas con la afiliación de Trabajadores Independientes (TI), Asegurados Voluntarios (AV) y Asegurado Migrantes en plataformas, recepción de solicitudes de estudio en plataformas, atención de las solicitudes por parte de jefaturas y de los Inspectores, adicionalmente, varias jefaturas de área tuvieron la iniciativa de adquirir el servicio de internet mediante enrutadores inalámbricos conocidos como MIFI´s, lo anterior con medios económicos propios.

Al respecto, se destaca la iniciativa de las jefaturas de esa Dirección, al tratar de minimizar el impacto en el desarrollo de las actividades sustantivas que tienen asignadas sus respectivas unidades, producto de la limitación de internet y acceso a los servicios habilitados mediante la web.

No obstante, este Órgano de Fiscalización y Control en su rol de asesor informa a la administración activa los aspectos esbozados en el presente oficio respecto a la implementación de redes inalámbricas de proveedores externos, mecanismos de seguridad mínimos a considerar, el análisis de beneficios y riesgos asociados a su uso y la respectiva aprobación por parte de las instancias superiores, lo anterior con el objetivo de que sean valorados y de considerarse oportuno se ejecuten las acciones que permitan minimizar los riesgos asociados a posibles brechas de ciberseguridad que sean aprovechadas por los cibercriminales para acceder a los datos de usuarios gestionados por la CCSS.

Atentamente,

**AUDITORÍA INTERNA**

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.15 15:06:04 -06'00'

Lic. Olger Sánchez Carrillo
**Auditor**

OSC/RJS/RAHM/GMP/lbc

C. Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera -1103.
Máster Idannia Mata Serrano, subgerente a.i., Dirección de Tecnologías de Información y Comunicaciones - 1150.
Auditoría.