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

AS-AATIC-103-2022
21 de junio de 2022

Doctora
Iliana Musa Mirabal, directora general
HOSPITAL DE GUAPILES - 2602

Estimada señora:

ASUNTO:	**Oficio de asesoría referente a la instalación de una red WIFI en el Dirección General del hospital Guápiles, con la finalidad de acceder a servicios web externos como contingencia por el ciberataque sufrido el 31 de mayo de 2022.**

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 aspectos relacionados con la instalación de una red WIFI de un proveedor externo en la Dirección General del hospital de Guápiles, con la finalidad de acceder a servicios web externos, a raíz de los ataques cibernéticos sufridos por la institución el pasado 31 de mayo del 2022, lo que provocó la suspensión de los sistemas y servicios informáticos institucionales de manera preventiva.

En consonancia con lo anterior, esta Auditoría procedió a visitar las instalaciones del hospital de Guápiles, con la finalidad de aplicar instrumento de verificación de afectaciones en los servicios como consecuencia de los ciberataques mencionados, en la cual se constató la instalación de un modem WIFI del proveedor Kolbi, el cual se encuentra en uso en la dirección general de ese centro médico.

I. ANTECEDENTES

El 20 de abril del 2022, el portal de Recursos Humanos sufrió un ataque cibernético, tal como lo informó el diario La Nación[1], en nota con el titular de “Portal de Recursos Humanos de CCSS sufre ataque cibernético”, indicando:

> *“Las plataformas digitales de las entidades públicas siguen siendo objeto de ataques cibernéticos. La Caja Costarricense de Seguro Social (CCSS) sufrió este miércoles una incidencia en su portal de Recursos Humanos, que obligó a activar una revisión integral de todos sus sistemas para determinar el alcance de lo ocurrido.*
>
> *El ingeniero Roberto Blanco Topping, director de Tecnologías de Información de la CCSS, detalló que una vez detectado el problema se procedió a blindar los accesos, dar de baja el portal y coordinar con los equipos técnicos para determinar si se produjo alguna extracción de información o de datos, o eventuales accesos a otras plataformas.*
>
> *“Los equipos de monitoreo, humanos y en conjunto con las herramientas tecnológicas con las que se cuenta detectaron incongruencias con respecto a la gestión de datos en el portal de Recursos Humanos de la institución y se determinó que se había producido un ataque externo”, detalló mediante un comunicado.*

Posteriormente, el 31 de mayo de 2022, se registró en horas de la madrugada un nuevo ciberataque contra los servidores de la C.C.S.S., el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

[1] Diario La Nación 20 de abril de 2022

En ese sentido, el Dr. Alvaro Ramos Chaves, presidente ejecutivo de la institución el 1 de junio del 2022, en conferencia de prensa a medios nacionales, mencionó:

> *"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"*

Aunado a lo anterior, el 6 de junio del 2022, se comunicó en el medio digital Crhoy, respecto al nivel de infección de institucional:

> *"La Caja Costarricense de Seguro Social* ***confirmó que el 67 por ciento de sus servidores se infectaron tras los ciberataques*** *de la semana pasada.*
>
> *La Dirección de Tecnologías de Información y Comunicaciones (DTIC) de la Caja está concluyendo la revisión de 27.755 computadoras en todo el país, de las cuales 9.600 se identificaron como infectadas, lo que significa el* ***27% del total de las terminales.***
>
> *De igual manera, se avanzó en la revisión de los 996 servidores de los cuales* ***773 fueron revisados, encontrándose 665 infectados que representa el 67%,*** *informó la institución." (lo resaltado corresponde al original)*

Como resultado de lo anterior y como medida de contención del ataque, se procedió a la desconexión de los sistemas como el Expediente Digital Único en Salud (EDUS), Sistema Central de Recaudación (SICERE), Portal Web, Sistema de Farmacia (SIFA), entre otros, además del apagado de los equipos de usuario final conectados a la red institucional, con la finalidad de proceder al diagnóstico de las afectaciones, así como a bajar los servicios de navegación web institucionales.

Adicionalmente, mediante oficio GA-CAED-0260-2022 del 02 de junio del 2022, suscrito por el Dr. Mario Vílchez Madrigal, director a.i., del Centro de Atención de Emergencias y Desastres, comunicó al cuerpo gerencial, directores de sede, directores de red integrada de servicios de salud, directores regionales de sucursales, directores generales y administrativos financieros de hospitales y directores y administradores de área de salud, la declaratorio de estado de emergencia institucional por los ciberataques, en lo que interesa indicó:

> *"- Que existe una Declaratoria de Emergencia Nacional en todo el sector público debido a los ciberataques que han afectado la estructura de los Sistemas de Información, mediante Decreto No. 43542-MP-MICITT.*
>
> *- Que la Caja Costarricense de Seguro Social, ha sido víctima de estos ciberataques, especialmente en la madrugada del día 31 de mayo del 2022.*
>
> *- Que de acuerdo con los informes presentados por la Dirección de Tecnologías de Información y Comunicaciones al Centro Coordinador de Emergencias Institucional (CCEI) se tuvo que realizarla desactivación controlada de los servicios TI institucionales el 31 de mayo del 2022.*
>
> *(…)*
>
> *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 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)."*

Finalmente, esta Auditoría ha tenido conocimiento de múltiples comunicados emitidos por la Dirección de Tecnologías de Información y Comunicaciones, relacionados con la atención de las afectaciones del ciberataque, en aspectos tales como; proceso de revisión de equipos de usuario local, procedimiento de revisión de servidores, procedimientos de limpieza de equipos, procedimientos de aplicación de Microclaudia, entre otros.

II. CONSIDERACIONES

En consonancia con lo anterior y dado que, producto del resultado del ciberataque sufrido el 31 de mayo de 2022, se procedió a la suspensión de los sistemas institucionales y los servicios de navegación web, como medida de protección temporal a efectos de contener la propagación del ramsomware, esta condición limita las acciones administrativas que requieren la consulta o modificación de datos en sitios web externos tales como: el SICOP.

La situación descrita pone en riesgo la oportuna atención de los diversos requerimientos de la contratación administrativa, lo que eventualmente compromete la continuidad del abastecimiento de bienes y servicios necesarios para la operación del centro médico.

Ante esa circunstancia, la dirección general de ese centro médico, con la colaboración de la Asociación para el Continuo Desarrollo del hospital de Guápiles, instaló un servicio de internet por medio de un enrutador WIFI que da servicios a esa dirección y a la dirección financiera administrativa.

Según lo indicado por la Dra. Iliana Musa Mirabal, directora, la mencionada asociación está a cargo del pago del servicio, además es utilizado para facilitar un canal de acceso a los portales web externos mencionados. Adicionalmente, la Dra. Musa Mirabal señaló que la red se encuentra oculta para los visitantes y cuenta con contraseña de acceso.

Respecto a la autorización por parte del nivel superior, mencionó que esta situación fue comunicada a la Gerencia Médica y a la Dirección de Red Integrada de Prestación de Servicios de Salud Huetar Atlántica en las diversas sesiones mantenidas mediante videoconferencia a raíz de la emergencia.

Aunado a lo anterior, esta Auditoría procedió a la verificación de la contraseña de acceso, la cual está construida por una palabra, un símbolo y dos números, esta configuración ciertamente tiene algún grado de seguridad, sin embargo, según buenas prácticas de seguridad sería vulnerable ante un ataque de diccionario[2].

Adicionalmente, se verificó la modificación de la contraseña de administrador del router inalámbrico, dado que se modificó la que por defecto establece el fabricante[3] .

Al respecto, el artículo 8 de la Ley General de Control Interno, respecto al sistema de control interno, establece:

> *"(…) 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."*

[2] La técnica consiste en probar consecutivamente muchas palabras reales recogidas en los diccionarios de los distintos idiomas, y también las contraseñas más usadas como "123456", para tratar de **romper las barreras de acceso a sistemas protegidos con clave**. Este tipo de ataque está basado en el hecho probado de que un **gran número de usuarios eligen las mismas contraseñas** fáciles de recordar, pero también fáciles de adivinar por parte de los delincuentes.
[3] Usuario: Admin; contraseña: admin

Además, las Normas Técnicas para la Gestión y Control de las Tecnologías de Información promulgadas por el Ministerio de Ciencia, Innovación, Tecnologías y Telecomunicaciones, en su apartado X "Desarrollo, implementación y Mantenimiento de Sistemas de Información, establece:

> "*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."*

Adicionalmente, en el apartado XI. Seguridad y Ciberseguridad, las normas citadas establecen:

> *"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 establecerlos 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, danos 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 instalación de redes inalámbricas, de proveedores externos eleva el riesgo de eventuales vulnerabilidades de seguridad, al no contar con monitoreo y otras herramientas institucionales que aseguren la prestación del servicio en las mejores condiciones, esta situación además se agravaría en caso de conectarse a equipos que pertenezca a la institución.

Es necesario indicar que aún en las condiciones actuales en las cuales las comunicaciones institucionales se han visto afectadas, deben ser consideradas las acciones que permitan asegurar que las instalación de redes o soluciones externas, cuentan con la autorización y coordinación de las autoridades correspondientes, además de la participación y colaboración del órgano técnico que permita asegurar que se cumplan con los requerimientos mínimos aceptables, en aspectos de seguridad, acceso y configuración entre otros, además del cumplimiento de las condiciones que se indican en la normativa vigente relacionadas con las donaciones que recibe el centro médico.

Aunado a lo anterior, se debe considerar la implementación de una contraseña con nivel mayor de complejidad, a efectos de impedir accesos no autorizados, o de prevenir las intrusiones que se han materializado en la red institucional.

Ciertamente, es destacable la iniciativa de este centro médico orientada a promover la continuidad del servicio y de disminuir los riesgos asociados a la atención inoportuna de procedimientos que requieren el acceso a sitios web de externos, se requiere mantener en la medida de las posibilidades el cumplimiento de la normativa vigente en materia de telecomunicaciones, así como de las coordinaciones y autorizaciones de los niveles jerárquicos correspondientes.

Debido a lo anterior, 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 realice una valoración de los aspectos señalados, y eventualmente se fortalezca las medidas de control interno sobre este particular.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.21 14:47:52 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AAM/ghc

C. Dra. Silene María Aguilar Orias, directora Dirección de Red Integrada de Prestación de Servicios de Salud Huetar Atlántica - 2699
Auditoría