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

AD-AATIC-074-2022
4 de julio de 2022

Doctor
Esteban Vega de la O, gerente
GERENCIA DE LOGISTICA – 1106

Doctora
Angie Cervantes Barrantes, líder usuaria
Sistema Integrado Laboratorio Clínico
DIRECCIÓN DE REDES INTEGRADAS PRESTACIÓN DE SERVICIOS DE SALUD REGIÓN CENTRAL SUR -2399

Estimadas señoras:

ASUNTO:	**Oficio de Advertencia sobre equipos de laboratorio pertenecientes a los contratos de laboratorio (CAPRIS-ROCHE) afectados por el ciberataque del 31 de mayo del 2022**.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y consecuente al oficio AI-874-2022 del 6 de junio del 2022, en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022, esta Auditoría tuvo conocimiento de los oficios GG-DTIC-2929-2022 y GG-DTIC-3067-2022, del 10 y 18 de junio del presente año, respectivamente, emitidos por la Dirección de Tecnologías de Información y Comunicaciones (DTIC), en los cuales se informa sobre la situación actual de los equipos de cómputo y servidores pertenecientes al contrato de Laboratorio (CAPRIS-ROCHE).

Al respecto, este Órgano Fiscalizador efectuó una revisión de las misivas supra citadas, evidenciando que la DTIC al 10 de junio del presente año, detectó[1] 21 sitios con equipos que tienen instalado el sistema operativo Microsoft Windows 7, el cual ya no recibe soporte por parte del fabricante desde enero del año 2020. A continuación, el detalle de los establecimientos de salud:

[1] Oficio DTIC-2929-2022 del 10 de junio suscrito por el Máster Roberto Blanco Topping, Subgerente a.i de Tecnologías de Información en ese momento y la Licda. Vanessa Carvajal Carmona, jefe de la subárea de seguridad de tecnologías de información.

Tabla 1:
DTIC: Centros de Salud con equipos con Windows 7
Al 10 de junio 2022

1. Hospital Monseñor Sanabria
2. Hospital San Rafael de Alajuela
3. Hospital México
4. Hospital San Juan de Dios
5. Hospital Nacional de Niños
6. Hospital Dr. Rafael Á. Calderón Guardia
7. Hospital San Vicente de Paúl
8. Hospital Máx Peralta
9. Hospital Enrique Baltodato
10. Hospital Escalante Pradilla
11. Hospital Guápiles
12. Hospital San Carlos
13. Hospital Tony Facio
14. Hospital de Upala
15. Centro Nacional de Rehabilitación (CENARE)
16. Hospital de Los Chiles
17. Hospital Psiquiátrico
18. Hospital La Anexión
19. Clínica Jimenez Nuñez
20. Hospital Nacional de las Mujeres
21. Clínica Dr. Marcial Rodríguez

Fuente: Auditoría Interna. Elaboración propia con base en oficio GG-DTIC-2929-2022.

Como se observa en la tabla anterior, la situación se presenta mayoritariamente en centros hospitalarios con un total de 18, así como, el CENARE y dos áreas de salud. Al respecto, señala la Dirección de Tecnologías de Información y Comunicaciones, que estos sitios ya fueron visitados por el contratista responsable, razón por la cual se presume los equipos fueron formateados, pero se les volvió a instalar la misma versión de Microsoft Windows 7.

Del mismo modo, según revisión de la consola de administración del software MicroClaudia[2] en España, la DTIC identificó 19 servidores y 24 equipos de laboratorio con el mismo nombre, pero diferente dirección IP (Internet Protocol por sus siglas en inglés). Sobre lo anterior, la DTIC señala que los expertos de la herramienta indican lo siguiente: *"(…) Es contraproducente ya que de contaminarse uno de esos servidores automáticamente se tendrían que deshabilitar todos los servidores, o bien equipos, por no saber a qué sitio corresponde, lo cual ocasionaría una afectación total para el servicio de Laboratorio correspondiente (…)".*

Por otra parte, en oficio GG-DTIC-3067, del 18 de junio del 2022, suscrito por la Licda. Vanessa Carvajal Carmona, jefe de la subárea de seguridad de tecnologías de información y enlace CCSS-MICITT-CNE, señala el apoyo solicitado a los centros de gestión informática (CGI) para que, en coordinación con la empresa correspondiente, se ejecuten las guías para la limpieza y formateo de los equipos pertenecientes a los contratos vigentes en los diferentes laboratorios clínicos.

[2] Es una capacidad basada en el motor de **CLAUDIA** que proporciona protección contra código dañino de tipo **ransomware** a los equipos de un organismo. Para ello, hace uso de un agente ligero para sistemas Windows que se encarga del despliegue y ejecución de vacunas. Tomado del sitio: https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html , el 22 de junio de 2022.

Pese a lo anterior, la misiva cita que existen reportes de servidores funcionando con la versión de sistema operativo Windows Server 2008, la cual no recibe soporte del fabricante y además incumple la *"Guía de formateo de Servidores 2"*. Adicionalmente, se identificaron equipos con Windows Server 2012 Estándar y R2, los cuales mantienen soporte extendido únicamente hasta octubre del 2023, ante esto, la DTIC autorizó mantenerlos con esa versión bajo la salvedad que a julio del 2023, sean debidamente migrados por el contratista a Windows Server 2016 o superior, esto en apego al análisis de las cláusulas del pliego cartelario y la responsabilidad del proveedor de ejecutar las actualizaciones correspondientes.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, en el apartado XI. Seguridad y Ciberseguridad, refiere lo siguiente:

> *"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 Proteccion 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 Proteccion 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 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."*

Ese mismo marco normativo, en el inciso XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, indica lo siguiente:

> *"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 Directriz N° 133-MP-MICITT del 21 de abril de 2022, del Presidente de la República, la Ministra de la Presidencia y la Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones, indica en sus artículos 2 y 6, lo siguiente:

> *"Artículo 2 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a realizar los procesos internos para promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica, sea que la misma corresponda a la Administración Pública directamente o esté contratada de manera total o parcialmente, incluyendo como mínimo actualizaciones permanentes de todos los sistemas institucionales, cambiar contraseñas de todos los sistemas institucionales (correos electrónicos, sistemas operativos, servidores, VPN, redes sociales, entre otros posibles), deshabilitar servicios y puertos no necesarios y monitorear la infraestructura de red, con el fin de garantizar que los eventos adversos relacionados con incidentes de ciberseguridad sean detectados, registrados y gestionados de forma que se pueda limitar el impacto de los mismos en cada institución o entidad. (El resaltado no corresponde al original)*
>
> *Artículo 6 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a que las alertas técnicas emitidas por el CSIRT-CR sean aplicadas, según corresponda en cada institución y sus sistemas, esto con el fin de disminuir las vulnerabilidades tecnológicas en las instituciones del país. Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a valorar la alerta técnica recibida y realizar los procedimientos respectivos para poder aplicarla dentro de su institución."*

La Guía *"Limpieza de PC infectados del usuario final versión 2"*, apartado *"Puntos por considerar"*, inciso 2 y 4, señala lo siguiente:

> *"2. Si el equipo de cómputo cuenta con sistema operativo Windows XP, Windows 7 o Windows Vista, deben apartarlo y no utilizar más ese equipo.*
>
> *4. Si el equipo de cómputo cuenta con sistema operativo Windows 8/8.1 se debe hacer la migración al sistema operativo Windows 10."*

La Guía *"Limpieza de Servidores Windows Infectados versión 3"*, en el punto 3, indica lo siguiente:

> *3. En caso de servidores Windows Server, se deben reinstalar con Windows Server 2016 Standard o superior; si cuentan con versiones anteriores y no es posible migrarlos; deben apartarlos, apagarlos y desconectarlos hasta que se instruya qué hacer.*

Al respecto, es significativo señalar que esta Auditoría desde el año 2019, mediante el producto AD-ATIC-1199-19, advirtió a la Administración Activa sobre la finalización del ciclo de vida para el soporte técnico del sistema operativo Microsoft Windows 7, evidenciando en ese ese momento alrededor de 5051 estaciones de trabajo a nivel institucional con esa versión.

De esta forma, la situación descrita implica la materialización de riesgos para recibir actualizaciones de seguridad en torno a la resolución de incidencias por parte de la empresa fabricante, por ende, sin el soporte técnico continuo de Microsoft, las instalaciones virtualizadas y físicas no pasarán ninguna auditoría de seguridad, provocando vulnerabilidades en el sistema operativo y sus aplicaciones, lo anterior debido a la ausencia de soluciones para las debilidades identificadas, las cuales previenen ataques informáticos por parte de hackers, virus u otro tipo de malware y que podría representar una de las causas del evento ocurrido el 31 de mayo del presente año.

En ese mismo orden de ideas, la ausencia de actualizaciones y parches críticos a nivel de software, limita la ejecución de nuevas funcionalidades, impidiendo una mayor estabilidad y rendimiento de los sistemas operativos, lo cual podría comprometer el adecuado funcionamiento de los equipos computacionales y generar eventualmente una afectación en el servicio brindado a los usuarios, además de incrementar las cargas de trabajo de los funcionarios destacados en tareas de soporte y mantenimiento de recursos de tecnologías de información.

Adicionalmente, mantener los equipos de laboratorios clínicos u otros en esa condición, podría incrementar el riesgo de un nuevo ciberataque, como el ocurrido el 31 de mayo del 2022, el cual ha generado un impacto significativo en la prestación de servicios de salud que se brinda a la población, por tanto, no acatar las directrices emitidas por la DTIC, para garantizar el adecuado funcionamiento y protección de los equipo, representa una omisión a principios de control interno asociados con las obligaciones de los titulares subordinados de tomar de inmediato medidas correctivas ante evidencia de desviaciones o irregularidades, siendo en este caso, de índole técnico, aspecto que eventualmente podría constituirse generador de responsabilidades de carácter administrativo, civil o penal.

Debido a lo anterior, en aras de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa y advierte para que realice una valoración de los aspectos señalados, y se ejecuten las acciones conforme derecho correspondan para subsanar en forma inmediata los riesgos expuestos en el presente documento.

Finalmente, se solicita informar a esta Auditoría Interna sobre las acciones a ejecutar obtenidas del análisis del presente documento en un **plazo de un mes**.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.04 14:16:33 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/EZCh/lbc

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva -110.2
Doctor Roberto Cervantes Barrantes, gerente, Gerencia General- 1100.
Doctor Randall Juárez Álvarez, gerente, Gerencia Médica-2901.
Máster Esteban Zúñiga Chacón, jefe, Centro de Gestión Informática, Gerencia Médica-2901
Máster Idannia Mata Serrano, subgerente a.i, Tecnologías de Información y Comunicaciones- 1150.
Licenciada Vanessa Carvajal Carmona, jefe, Subárea Seguridad de Tecnologías de Información- 1150
Auditoría