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

AS-AATIC-198-2022
12 de octubre de 2022

Doctor
Randal Alvarez Juárez, gerente
GERENCIA MÉDICA-2901

Doctor
Esteban Vega de la O, gerente
GERENCIA LOGÍSTICA-1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS-1107

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

Ingeniero
Ronald Ávila Jiménez, director
DIRECCIÓN EQUIPAMIENTO INSTITUCIONAL-3110

Estimados(a) señores(a):

ASUNTO: Oficio de Asesoría sobre ciberseguridad para dispositivos y equipos médicos.

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre el impacto en la prestación de servicios de salud y la importancia de la ciberseguridad para dispositivos y equipos médicos en el contexto actual, producto del ataque cibernético en la plataforma tecnológica institucional, a partir del 31 de mayo del 2022, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa administración activa.

Al respecto, los resultados obtenidos son los siguientes:

I. ANTECEDENTES

El 31 de mayo de 2022, se registró en horas de la madrugada un ciberataque contra los servidores de la C.C.S.S., el cual obligó a realizar una desactivación controlada de los servicios TI institucionales, de acuerdo con los informes presentados por la Dirección de Tecnologías de Información y Comunicaciones al Centro Coordinador de Emergencias Institucional (CCEI).

Asimismo, en el contexto del presente oficio, es importante señalar que, de acuerdo con la norma ISO 14971:2007 "*Aplicación de la gestión del riesgo a los dispositivos médicos y reactivos de diagnóstico in vitro"*, un dispositivo médico es:

"Cualquier instrumento, aparato, dispositivo, equipo, implante, reactivo o calibrador para diagnóstico in vitro, programa informático, material u otro similar o relacionado, utilizado sólo o en combinación, destinado por el fabricante a ser utilizado en seres humanos con fines de:

- *Diagnóstico, prevención, control, tratamiento o alivio de una enfermedad.*
- *Diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia.*
- *Investigación, sustitución o modificación de la anatomía o de un proceso fisiológico.*
- *Mantenimiento o prolongación de la vida.*
- *Regulación de la concepción.*
- *Desinfección de dispositivos médicos.*
- *Proporcionar información para fines médicos mediante análisis in vitro de muestras derivadas del cuerpo humano.*

Y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios".

II. RESULTADOS OBTENIDOS

En la actualidad, muchas personas y centros hospitalarios, a nivel mundial, usan dispositivos médicos (con componentes electrónicos e informáticos) tales como bombas de insulina, marca pasos, neuroestimuladores, entre otros, que permiten un tratamiento eficiente y focalizado sobre los pacientes, mejorando su condición de salud y aumentando la capacidad de monitorización y seguimiento por parte de los médicos.

En materia de dispositivos y equipos médicos, la introducción tecnológica permitida por la conectividad y por el Internet de las cosas IoT (Internet of Things), se ha traducido en enormes ventajas, para los pacientes y su entorno familiar y confirman retadores campos de aplicación para beneficio de la humanidad, que generan una esperanza de encontrar soluciones a muchas de las enfermedades existentes y posiblemente anticipar la aparición de nuevas, ejemplo de esto es: Los recientes diagnósticos médicos asistidos por algoritmos de inteligencia artificial, los brazos robóticos para adelantar cirugías de alta precisión, implantes cocleares inteligentes, entre otros adelantos.

Las tecnologías conectadas permiten combinar los datos de pacientes y equipos provenientes de una amplia gama de dispositivos terapéuticos y de monitorización, sistemas de información clínica y otras fuentes utilizadas para la toma de decisiones. En una visita promedio al hospital, un usuario puede estar en contacto con hasta diez dispositivos médicos interconectados entre sí.

Algunos de los dispositivos médicos en red utilizados en hospitales y centros de salud, son nuevos, pero otros son antiguos y no disponen de protecciones de ciberseguridad o funcionan con sistemas operativos no soportados o descontinuados por el proveedor. Este escenario ofrece a los atacantes las mejores condiciones para acceder a los datos de salud o incluso para realizar ataques de movimiento lateral de la red.

De conformidad con lo anterior, se considera necesario analizar aspectos relevantes en materia de dispositivos y equipos médicos, así como, algunas de las normas, directrices y buenas prácticas de seguridad establecidas para la fabricación, uso y comercialización de éstos.

2.1 Ciberseguridad en dispositivos médicos

En nota informativa publicada, el 10 de mayo de 2022, en el sitio digital de PROCOMER, se hace mención a una encuesta denominada *"Medical Device Cybersecurity: Trends and Predictions 2022 Survey Report"* publicada por la empresa Cybellum, especializada en seguridad de tecnología médica, la cual respalda la opinión de que existe margen para que la industria de dispositivos médicos eleve los estándares de ciberseguridad.

Esta encuesta global se aplicó a 150 empresas de dispositivos médicos, indicándose dentro de los resultados más relevantes, lo siguiente:

> *"(…) en promedio, el 46% de los encuestados consideran cumplir con los estándares y regulaciones de ciberseguridad asociados a sus productos. La mayoría de encuestados tiene planes de cumplir con los requisitos de seguridad, pero esto podría tomar hasta 2023 o más tarde para que algunas empresas ajusten sus prácticas a las reglas. Los principios y prácticas de ciberseguridad del Foro Internacional de Reguladores de Dispositivos Médicos (IMDRF, por sus siglas en inglés) son la máxima prioridad para 2022. El 52% señaló como objetivo cumplirlas este año y un 37% de los encuestados considera que ya lo hace.*
>
> *Los resultados de la encuesta llegan inmediatamente después de la publicación del borrador de la guía de seguridad cibernética de la FDA. Sin embargo, el 78% de los encuestados indicó que su objetivo general es hacer lo mínimo necesario para lograr el cumplimiento de la FDA y la IMDRF. El hallazgo contrasta con el hecho de que el 83% señalara la seguridad de los dispositivos como una ventaja competitiva, pero está en línea con que el 80% ve la seguridad de los dispositivos como un "mal necesario" impuesto por los reguladores y con que el 79% prioriza el tiempo de comercialización sobre seguridad.*
>
> *Otro de los hallazgos señala que los encuestados tienen más efectivo que nunca para lograr esos objetivos, con un 50% de las empresas aumentando sus presupuestos de seguridad en al menos un 26%. Después de haber realizado las inversiones, el 99% de los encuestados tenía al menos algo de confianza en su capacidad para manejar un ataque cibernético. No obstante, la encuesta indica que el hecho de que el 65% pruebe el firmware de su dispositivo una vez al mes, como máximo, sugiere que las empresas pueden ser más vulnerables de lo que creen".*

Asimismo, dentro de las implicaciones para Costa Rica, según investigación realizada por PROCOMER (señalada en el mismo texto), se indicó que:

> *"(…) el 22% del sector TICS en Costa Rica ofrece servicios basados en tecnologías 4.0, con dispositivos médicos como el segundo principal sector de clientes de bienes.*
>
> *Adicionalmente, el 23% de las empresas del sector TICS vinculadas con tecnologías 4.0., ofrece servicios relacionados con ciberseguridad.*
>
> *Es importante que las empresas que ofrecen soluciones de ciberseguridad y con interés en la vertical de clientes de dispositivos médicos, estén al tanto de los requerimientos y estándares que estos deben implementar acorde a lo establecido en el IMDRF y la FDA, con el objetivo de que sus servicios se ajusten a las necesidades de la industria.*

> *Lo anterior, sobre todo porque según el artículo, más de la mitad de los encuestados todavía está en proceso para cumplir con dichos estándares solicitados (...)"*

En relación con lo anterior, en nota periodística publicada, el 13 de mayo de 2022, en el sitio digital saludiario.com, respecto a la guía de seguridad cibernética de la FDA, señaló:

La importancia de proteger los dispositivos médicos, según lo indicado por la FDA:

El borrador de la guía de seguridad cibernética de la Administración de Drogas y Alimentos de EE. UU (FDA), *"Seguridad cibernética en dispositivos médicos: consideraciones del sistema de calidad y contenido de las presentaciones previas a la comercialización"*, busca enfatizar la importancia de proteger los dispositivos médicos a lo largo del ciclo de vida de un producto.

Sobre la guía, la FDA en el aviso del Registro Federal indicó, lo siguiente:

> *"Estas recomendaciones pueden facilitar un proceso de revisión previo a la comercialización eficiente y ayudar a garantizar que los dispositivos médicos comercializados sean lo suficientemente resistentes a las amenazas de seguridad cibernética".*

¿Por qué es importante?

La ciberseguridad, particularmente en lo que respecta a los dispositivos médicos, ha adquirido una mayor importancia a medida que más pacientes se benefician de la atención conectada.

La FDA en su borrador de guía, señaló:

> *"La mayor conectividad ha dado como resultado que los dispositivos individuales funcionen como elementos únicos de sistemas de dispositivos médicos más grandes (…)".*

> *"Estos sistemas pueden incluir redes de centros de salud, otros dispositivos y servidores de actualización de software, entre otros componentes interconectados (…)"*

Asimismo, en publicación *"Seguridad y ciberseguridad en los dispositivos médicos"* efectuada por la Revista Sistemas (realizada por la Asociación Colombiana de Ingenieros de Sistemas), se indicó:

Sobre este tema, en los Estados Unidos de Norteamérica (EE. UU) y Europa, se han establecido muchas de las normas y buenas prácticas, con el fin de aumentar la protección y responsabilidad de los proveedores y prestadores de servicios de salud, tales como:

- *HIPAA (US Health Insurance Portability and Accountability Act).*
- *HITRUST (Health Information Trust Alliance).*
- *COBIT 5.0*
- *CIS Critical Security Controls (Center for Internet Security).*
- *ISO 27002*
- *NIST Cybersecurity Framework.*

- *GDPR (General Data Protection Regulation).*
- *Indicaciones de protección y aseguramiento de la FDA[1] (Food & Drug Administration EE. UU).*

"En concreto y de manera general la FDA recomienda:

- *Identificar activos, amenazas y vulnerabilidades, y evaluar su impacto en la funcionalidad de los dispositivos y en los usuarios/pacientes finales.*
- *Evaluar la probabilidad de que una amenaza y una vulnerabilidad sean explotadas. Esto puede lograrse utilizando herramientas de evaluación de vulnerabilidad de ciberseguridad.*
- *Determinar los niveles de riesgo y las estrategias de mitigación adecuadas; por ejemplo, la FDA recomienda que los fabricantes determinen el "nivel de alerta" apropiado para el software (es decir, una estimación de la gravedad de las lesiones que un dispositivo podría permitir o infligir, directa o indirectamente, a un paciente u operador, como resultado de fallos del dispositivo, defectos de diseño, o empleando el dispositivo para su propósito previsto). Los niveles de preocupación varían desde Mayor (riesgo grave de muerte o lesión), Moderado (lesión menor) o Menor (improbable que cause lesión).*
- *Evaluar el riesgo residual en función de criterios adecuados de aceptación del riesgo. Limitar el acceso a los dispositivos a usuarios de confianza mediante el uso de programas de autenticación, tiempos de espera, privilegios de autorización por capas (por ejemplo, proveedor, administrador del sistema) y cierres de sesión.*
- *Restringir las actualizaciones de software o firmware basado en código autenticado y asegurar que los datos puedan transferirse de forma segura desde y hacia el dispositivo médico, por ejemplo, mediante cifrado.*

(…) de forma complementaria, la TGA[2] (Australian Therapeutic Goods Administration), establece un conjunto de principios esenciales para la fabricación, uso y comercialización de dispositivos médicos, que brindan tanto a los proveedores como a las clínicas, un marco de responsabilidad demostrada y cumplimiento respecto de los retos de seguridad y control, los cuales se desarrollan en una extensa lista de chequeo encabezada por los siguientes fundamentos básicos:

- *El uso de los dispositivos médicos (implantados o no) no debe comprometer la salud ni la seguridad del paciente ni del operador.*
- *El diseño y construcción de dispositivos médicos debe hacerse de acuerdo con los principios de seguridad en el ámbito físico y lógico.*
- *Los dispositivos deben ser desarrollados para el uso previsto.*
- *La seguridad (física y lógica) del dispositivo debe ser una característica de largo plazo.*
- *Los dispositivos médicos no deben verse afectados negativamente por el transporte o el almacenamiento.*
- *Los beneficios del uso de los dispositivos médicos deben compensar cualquier efecto indeseable (...)".*

[1] FDA: Administración de Drogas y Alimentos de EE. UU.
[2] TGA: Administración Australiana de Productos Terapéuticos

En consecuencia, sin la correcta implementación de los requerimientos, estándares y buenas prácticas establecidas a nivel mundial, para la fabricación, uso y comercialización de dispositivos médicos, aumenta el riesgo de que, ante un eventual ciberataque, se comprometa la seguridad y/o efectividad de éstos, repercutiendo en la calidad y oportunidad de la atención médica y la vida de los pacientes (una falla técnica, podría producir una alteración orgánica o incluso la muerte).

2.2 Riesgos:

Según informe desarrollado por un grupo de investigadores de ciberseguridad de la compañía Palo Alto Networks, es posible hackear los marcapasos (pacemakers), bombas de insulina con bluetooth y otros dispositivos implantados conectados a Internet.

Cabe destacar que los dispositivos de uso médico no son dispositivos de control tradicionales como pueden serlo las máquinas herramienta, al no disponer de los PLC [3]ni RTU[4] habituales. Su tipología implica que no se puedan aplicar medidas de seguridad generales, sobre todo en lo referente a actualizaciones y parcheos, o ejecución de copias de seguridad, por ejemplo.

Según el citado informe, los 5 dispositivos médicos más vulnerables a los hackers en un hospital son:

- **Equipos de mamografía**

Estos dispositivos médicos son administrados por computadoras a través de un firmware, y solo los técnicos que tienen acceso a la administración pueden hacer ajustes, incluyendo el cambio de contraseñas. Como tal, todo lo que un hacker necesita hacer es obtener acceso a la contraseña y reprogramar el dispositivo para proporcionar lecturas inexactas.

- **Dispositivos cardíacos**

Una de las principales razones por las que los marcapasos y dispositivos similares contienen tantas vulnerabilidades se debe principalmente al hecho de que muchos proveedores compran componentes de terceros para su software o hardware.

- **Máquinas de imágenes por resonancia magnética**

Estos dispositivos son relativamente fáciles de atacar ya que muchos sistemas mantienen sus contraseñas predeterminadas.

- **Desfibriladores implantados**

Además de los marcapasos, también se sabe que los desfibriladores implantados tienen vulnerabilidades de seguridad. Se utilizan para controlar la actividad eléctrica de un corazón y pueden ser monitoreados a través de transmisores de radio.

[3] PLC: Controlador Lógico Programable, más conocido (Programmable Logic Controller, debido a sus siglas en inglés) es básicamente una computadora que se utiliza en la ingeniería de automatización para las industrias, es decir, para el control de la maquinaria de una fábrica o de situaciones mecánicas.
[4] Una RTU es un equipo instalado en una localidad remota que recopila datos y luego la codifica en un formato que le permita transmitirlos hacia una estación central (Master Terminal Unit, MTU) u otra RTU.

- **Bombas de insulina**

Los marcapasos y los desfibriladores no son los únicos dispositivos médicos de debate, las bombas de insulina también se han encontrado ser vulnerables a la piratería debido a los principales errores de seguridad. El paciente podría sufrir hasta una sobredosis si un hacker accede a estas bombas.

Las amenazas de ciberseguridad para el sector de la salud se han vuelto más frecuentes, graves e impactantes desde el punto de vista clínico, éstos han dejado inoperables los dispositivos médicos y las redes hospitalarias, interrumpiendo o retrasando el oportuno diagnóstico, tratamiento y atención del paciente, por ejemplo: En Alemania ocurrió un impactante y lamentable evento, ocasionado por un ataque de ransomware (que paralizó toda la red informática de un hospital), lo que obligó al personal de salud a dirigir los pacientes a otros centros médicos, dando como resultado que, una mujer que requería atención de emergencia por una enfermedad que amenazaba su vida: murió, después de tener que ser trasladada a otra ciudad para recibir tratamiento.

2.3 Referente a la adquisición de equipo médico en la CCSS.

Según datos extraídos de la *Memoria Institucional 2021 de la CCSS*, el eje estratégico de Infraestructura y Equipamiento en la institución se ha enfocado hacia la continuidad de la ejecución del Portafolio Institucional de Proyectos de Infraestructura y Equipamiento, principalmente en infraestructura hospitalaria, el mantenimiento de los centros de salud y **equipo médico**.

En el citado documento del 2021, se indicaron los siguientes proyectos de infraestructura y dotación de equipamiento de punta:

Infraestructura y equipamiento:

> ***"(…) Once obras nuevas entregadas y en operación que representan ₡62.629 millones:***
>
> *Salas de operaciones, sala de partos y unidad de cuidados intensivos del hospital México, Centro Psiquiátrico Penitenciario, sede de área de salud de Santa Cruz de Guanacaste, dos EBAIS en Talamanca (Bajo Blei y Piedra Mesa), Diálisis Peritoneal y Hemodiálisis hospital Enrique Baltodano, Liberia, rehabilitación de los módulos de lavandería, casa máquinas y proveeduría en el hospital Tomas Casas Casajús, angiógrafo y mamógrafo hospital San Vicente de Paúl, Heredia; 32 ultrasonidos radiológicos, cinco ultrasonidos gineco-obstétricos y sistema fotovoltaico en el puesto de visita periódica Isla Caballo. Dichas obras significan 43.024 m2 nuevos con última tecnología.*
>
> ***Diecisiete proyectos en ejecución de contratos por un costo de ₡267.321 millones:***
>
> *Nuevas sedes hospitales William Allen, Turrialba y Monseñor Sanabria, Puntarenas, Servicio Conjunto de Atención del Cáncer, reforzamiento estructural y readecuación de Oficinas Centrales, sustitución de gamma cámara por SPECT/CT hospital México, reposición tomógrafos hospitales nacionales, rayos X Clínica Carlos Durán, remodelación y ampliación del servicio de Anatomía Patológica, hospital México y el servicio de Hemodinamia del hospital San Rafael de Alajuela.*

29 proyectos en etapa de contratación:

¢97.231 millones invertidos en el 2021, para pagos de proyectos concluidos y en ejecución.

52 proyectos están en diseño, estudios y adquisición de terrenos mediante la modalidad de Fideicomiso Inmobiliario CCSS y Banco de Costa Rica, (30 áreas de salud, 18 sucursales y 04 direcciones regionales de sucursal), que en conjunto significan $583,7 millones en inversión.

Torre La Esperanza hospital Nacional de Niños (Fideicomiso con Banco Nacional). Se adquirieron tres terrenos ya a nombre de la CCSS.

Nuevo hospital de Cartago, se realizó la publicación de la licitación (…)".

Equipo médico:

"(…) Equipos entregados:

- *Angiógrafo hospital de Heredia.*

  Inversión: ¢2.194 millones.
  Monto ejecutado en el 2021: ¢2.111 millones.
  Finalizado de forma satisfactoria y entregado a la unidad usuaria para la puesta en marcha que ha resultado exitosa, impactando directamente en la administración para bajar las listas de espera de pacientes.

- *Treinta y dos ultrasonidos radiológicos instalados y funcionando, en los siguientes centros de salud:*

  ***Cinco** en hospital México, **cuatro** en hospital San Vicente de Paúl, **dos** en hospital Niños, **ocho** en hospital Calderón Guardia, **dos** en hospital San Juan de Dios y **dos** para el hospital Tony Facio.*

  ***Uno** en área de salud de Coronado, área de salud Desamparados, Hospital de Guápiles, área de salud Tibás Uruca-Merced (Cl. Clorito Picado), hospital Los Chiles, hospital Valverde Vega, hospital Max Peralta, hospital La Anexión y hospital Tomas Casas.*
  Inversión: ¢1.428 millones.

- *Cinco ultrasonidos Gineco- Obstétricos equipos instalados y funcionando en los siguientes centros:*

  ***Dos** en el hospital México y **uno** en el hospital las Mujeres, hospital Dr. Carlos Luis Valverde Vega y el CAIS Cañas.*
  Inversión: ¢268 millones.

  Proyectos de equipamiento en ejecución:

- *Gama cámara SPET-CT hospital México.*

Área: 261 m2.
Costo total estimado: ¢1.508 millones.
Monto ejecutado en el 2021: ¢1.308 millones.

Equipo adquirido e instalado. Pendiente de permisos del Ministerio de Salud para pruebas de funcionamiento.

- *Reposición tomógrafos hospitales nacionales (hospital México).*

  Área: 907 m2.
  Costo total estimado: ¢3.762 millones.
  Monto ejecutado en el 2021: ¢380 millones.
  Se avanzó un 60% en el proceso de construcción y equipamiento. El 9 de julio del 2021 se emitió orden de inicio de los ítems de construcción y equipamiento.

- *Reposición tomógrafos hospitales nacionales (hospital San Juan de Dios).*

  Área: 702 m2.
  Costo total estimado: ¢3.613 millones.
  Se avanzó un 2% en el proceso de construcción y equipamiento. Se iniciaron las obras, con la desinstalación del equipo de tomografía actual y demoliciones menores en los espacios a intervenir.

- *Reposición tomógrafo, hospital Dr. Rafael Ángel Calderón Guardia.*

  Área: 73 m2.
  Costo total estimado: ¢1.467 millones.
  Se logró obtener los permisos y visados. En la revisión por parte de las instituciones pertinentes para la obtención de los permisos de construcción para iniciar las obras.

- *Rayos X Clínica Carlos Durán.*

  Área: 67 m2.
  Costo total estimado: ¢492 millones.
  Monto ejecutado en el 2021: ¢79 millones.
  Logró un 28% avance acumulado de la construcción y equipamiento (…)".

Asimismo, en nota periodística publicada por el medio digital Delfino.cr el 02 de marzo de 2022, se indicó:

"El gobierno del Japón destinó $2.88 millones a favor de la Caja Costarricense de Seguro Social (CCSS). El monto se tradujo en la entrega de 161 equipos médicos que beneficiarán a más de 40.000 personas anualmente, en 36 centros médicos de todo el país.

En total son 91 monitores de signos vitales, 44 camas de hospital y 26 rayos x móviles, equipamiento clave para reforzar la capacidad de los servicios de salud nacionales, especializados, regionales y periféricos. La donación se dio con el objetivo de atender las necesidades de los pacientes afectados por la pandemia de la COVID-19 y así aliviar parcialmente la carga administrativa que ha enfrentado el sistema de salud público en los últimos dos años.

El proceso se hizo a través del Proyecto de Mejora del Sistema de Salud mediante la Provisión de Equipos Médicos y el proceso de adquisiciones gestado por la Oficina de Naciones Unidas de Servicios para Proyectos (UNOPS) en Costa Rica. El embajador del Japón en Costa Rica, Shinjiro Komatsu, señaló que el proyecto dio inicio el año anterior con el fin de reconocer la labor de las instituciones y el personal de salud en la crisis ocasionada por la COVID-19, y agregó:

Me alegra mucho saber que pudimos superar la cantidad de equipos médicos entregados en las diferentes provincias del país, a los distintos establecimientos de salud. Reconocemos la necesidad de contar con servicios de salud estables y por ello, para el pueblo japonés siempre será un honor cooperar con instituciones tan valiosas como la Caja Costarricense de Seguro Social".

Según señalaron vía comunicado de prensa, en el proceso de compra UNOPS lanzó tres licitaciones de forma simultánea, en las que participaron 32 oferentes, mayoritariamente de origen costarricense y la entrega del equipamiento médico se concretó dentro del plazo previsto, incluso a pesar de la crisis de abastecimiento en equipo médico que desató la pandemia (…)".

Asimismo, en medio digital Seminario Universitario del 17 de marzo de 2022, se informó:

"La Caja invirtió alrededor de ¢15 mil millones en la compra de más de 3.000 equipos médicos en 2020, para hacer frente a la pandemia por el COVID-19.

La Caja Costarricense de Seguro Social (CCSS) invertirá ¢600.000 millones de su presupuesto en equipos de tecnología de avanzada, mobiliario e infraestructura en los próximos 10 años, anunció hoy el presidente ejecutivo de la institución Román Macaya.

Según Macaya, esta inversión es parte de un portafolio de 348 proyectos para el periodo 2021-2030, y que implica una inversión total de ¢2 billones de colones, se informó mediante un comunicado de prensa.

Este año se planea invertir ¢18.500 millones en compras de nuevos equipos y tecnología, se indicó.

Por ejemplo, el próximo 30 de abril se recibiría un angiógrafo (equipo que emite rayos X y permite observar los vasos sanguíneos) y un mamógrafo para el Hospital San Vicente de Paul, en Heredia, estaría lista la readecuación de infraestructura para que funcione el nuevo servicio de hemodinamia (para realizar estudios de la sangre a través del sistema vascular).

Durante el 2020 la Caja invirtió alrededor de ¢15 mil millones en la compra de más de 3.000 equipos médicos, para hacer frente a la pandemia por el COVID-19., entre los que se pueden mencionar ventiladores pulmonares, bombas de infusión, camas, cánulas, rayos X, carros para transporte de insumos, aspiradores para secreciones, monitores de signos vitales, videolaringoscopios y artefactos como termómetros infra rojos sin contacto.

Según datos provistos por la institución a fines del año pasado, la CCSS estimó en ¢125 mil millones las compras realizadas por la institución durante el 2020, para atender la pandemia por C OVID-19".

De la información anteriormente expuesta, se observa que, institucionalmente se han hecho enormes esfuerzos administrativos y financieros para la dotación de equipos y dispositivos médicos de alta tecnología para la prestación de los servicios de salud en las diferentes regiones del país, siendo relevante el fortalecimiento de las medidas de ciberseguridad y la implementación de mejores prácticas desarrolladas a nivel mundial en este tema, con el fin de garantizar de manera razonable la protección de la información clínica y confidencial de los pacientes, así como la continuidad del servicio ante cualquier irrupción.

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.
d) Cumplir con el ordenamiento jurídico y técnico(...)"

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

"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."

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el Apartado XI, Seguridad y Ciberseguridad, 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 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 (…)".

III. CONSIDERACIONES

En la actualidad, los dispositivos y equipos médicos se convierten en herramientas novedosas y un medio para que la medicina y la tecnología se unan con el fin de generar nuevas oportunidades y soluciones, tanto para los pacientes como para las instituciones que brindan servicios de salud.

El sector salud se ha convertido en objetivo de los ciberatacantes, dada su poca madurez y experiencia en ciberseguridad en este tipo de equipos y dispositivos médicos, así como de su compleja infraestructura de operaciones.

Los atacantes, tras acceder a través de dispositivos y equipos médicos con acceso remoto, pueden aprovechar sistemas vulnerables y sin mantenimiento para infiltrarse en la red del hospital, pasar a otros dispositivos y sistemas conectados e instalar ransomware o malware.

En razón de lo anterior, es importante que los prestadores de servicios de salud y proveedores de dispositivos y equipos médicos (tecnológicamente modificados), valoren dentro de sus estrategias de fortalecimiento de los mecanismos de control, aquellos estándares, regulaciones y buenas prácticas de ciberseguridad establecidas a nivel mundial, así como, la concientización de los usuarios sobre los riesgos existentes en dicha materia, ya que una intrusión o ciberataque, podría afectar la funcionalidad y efectividad de estos dispositivos, repercutiendo de forma negativa en la salud de los usuarios.

De conformidad con lo expuesto, y en apego al artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones que se ejecuten, resulta fundamental que la administración activa se mantenga vigilante de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias, a fin de garantizar razonablemente la continuidad de los servicios de salud y el fortalecimiento de la gestión TIC en los centros de salud institucionales.

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio, con el objetivo de incentivar la capacidad de la Institución para recuperar y restablecer el componente TI después de la interrupción en sus sistemas de información debido al ciberataque del 31 de mayo de 2022.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.10.12 16:45:42 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/AEBB/lbc

C. Magister Marta Eugenia Esquivel Rodríguez, presidenta, Presidencia Ejecutiva -1102.
Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100.
Doctor Taciano Lemos Pires, director, hospital Dr. Rafael Angel Calderón Guardia -2101.
Doctora María Eugenia Villalta Bonilla, directora, hospital San Juan de Dios -2102.
Doctora Olga Arguedas Arguedas, directora, hospital Nacional de Niños Dr. Carlos Sáenz Herrera -2103.
Doctor Douglas Montero Chacón, director, hospital México-2104.
Doctor José Miguel Villalobos Brenes, director, hospital de las Mujeres Dr. Adolfo Carit-2105.
Doctora Milena Bolaños Sánchez, directora, hospital Nacional de Geriatría y Gerontología Dr. Raúl Blanco Cervantes-2202.
Doctor Roberto Aguilar Tassara, director, Centro Nacional de Rehabilitacion-2203.
Doctor Cristian Eugenio Elizondo Salazar, director a.i, hospital Nacional Psiquiátrico-2304.
Doctor Arturo Borbón Marks, director, Dirección Red Integrada de Prestación de Servicios de Salud Brunca-2799.
Doctora Olga Marta Chaves Pérez, directora a.i, Dirección Red Integrada de Prestación de Servicios de Salud Central Norte-2299.
Doctor Alberth Francisco Méndez Vega, enlace, Dirección Red Integrada de Prestación de Servicios de Salud Central Sur-2399.
Doctor Warner Picado Camareno, director, Dirección Red Integrada de Prestación de Servicios de Salud Chorotega-2599.
Doctora Silene Aguilar Orias, enlace, Dirección Red Integrada de Prestación de Servicios de Salud Huetar Atlántica-2699.
Doctor Juan Ignacio Rojas Bruno, enlace, Dirección Red Integrada de Prestación de Servicios de Salud Huetar Norte-2499.
Doctor Wilburg Díaz Cruz, director, Dirección Red Integrada de Prestación de Servicios de Salud Pacífico Central-2598.
Auditoría