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

AS-AATIC-174-2022
17 de agosto de 2022

Doctor
Randal Alvarez Juárez, gerente
GERENCIA MÉDICA-2901

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

Estimado(a) señor(a):

ASUNTO: Oficio de Asesoría sobre ciberseguridad hospitalaria.

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 hospitalaria 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).

II. RESULTADOS OBTENIDOS

La digitalización del sector de la salud sigue avanzando, la mayoría de los centros médicos u hospitalarios mantienen una actividad constante de 24x7 los 365 días del año, dependiendo cada vez más de sistemas de información para llevar a cabo los procesos administrativos, clínicos y diagnósticos (la mayoría de los equipos y medios de diagnósticos modernos que utiliza la medicina tienen un alto componente informático).

Si bien esta transformación digital conduce a mejores resultados en la atención de salud, como experiencias de pacientes más personalizadas y operaciones más optimizadas, también existe el potencial de aumentar los riesgos de seguridad. Toda esta red de dispositivos, equipamientos y sistemas conforman un entorno crítico y complejo de controlar, generando una oportunidad para el acceso de ciberdelincuentes a la información clínica de los pacientes.

2.1 Riesgos:

Los ataques a centros hospitalarios buscan el robo y comercialización de los registros médicos para venderlos o pedir rescates. Estos están llenos de información sensible que revela una imagen de todo el ciclo vital de una persona como datos personales, historial médico, financiero, direcciones de trabajo y hogar, entre otros. Sin embargo, las consecuencias de un ciberataque a un hospital no se limitan al robo o filtración de información médica, sino que conllevan otros riesgos relacionados con la práctica clínica y operacional de estas organizaciones.

Es importante recordar que la información clínica de un paciente es altamente sensible y el robo y/o mal uso de esta tiene serias consecuencias para la propia seguridad del paciente.

Los registros médicos pueden alcanzar un valor en el mercado negro entre 50 y 500 dólares, según el informe realizado por el instituto SANS (SysAdmin Audit, Networking and Security) y la empresa Norse (consultora privada que se especializa en seguridad y soluciones anti-fraude en la web.

Además, el citado informe de ciberseguridad, indica que, durante el 2020 se detectaron 50 mil ataques dañinos contra organizaciones dedicadas al sector de la salud, 375 de ellos exitosos.

A continuación, se indican, algunos antecedentes de ataques en el sector salud a nivel mundial:

- El 12 de mayo de 2017, el Sistema Nacional de Salud del Reino Unido (NHS por sus siglas en inglés) informó que 684 de sus organizaciones fueron atacadas por medio de un ransomware, incluidos los grupos de prácticas generales, hospitales y laboratorios. Se estima que tuvieron que cancelar 19 mil citas.
- Cuatro años después, el Health Service Executive- o HSE de Irlanda, también fue atacado por un grupo delictivo de ransomware. El resultado final para el HSE en Irlanda fue muy similar al del NHS en el Reino Unido, y el gobierno irlandés estima que los daños están en el rango de decenas de millones de euros.
- En septiembre de 2020, un ataque dirigido al Servicio de Salud en Alemania fue la causa de la muerte de una paciente que necesitaba atención de emergencia. El ataque paralizó el centro médico y por eso tuvo que ser trasladada a otra ciudad y no pudo ser tratada a tiempo.
- En los EE. UU, el mismo ransomware que ha afectado al sistema de salud irlandés, fue el responsable de ataques a 16 redes de atención médica y de primeros auxilios. En total, el grupo criminal ha sido responsable de paralizar a más de 400 organizaciones de atención médica en todo el mundo y exigen rescates de hasta $25 millones en algunos casos.

Según lo indicado por el medio digital elEconomista.es en nota periodística del 09 de marzo de 2021, para protegerse ante las amenazas cibernéticas, el sector sanitario ha invertido en ciberseguridad de manera acumulada 55 mil millones de euros en los últimos 5 años a nivel mundial. Esta cifra adquiere otra dimensión si se compara con los 50 mil millones de dispositivos médicos que estarán en uso globalmente en 2028, y que son susceptibles de sufrir algún tipo de ataque o manipulación por parte de los ciber delincuentes.

Con el paso del tiempo, el número de aplicaciones incluidas en los dispositivos médicos también aumentarán, por lo que el perfil de los requisitos para un software de seguridad apropiado podría cambiar y ser cada día más exigentes, los cortafuegos y el software de seguridad (antivirus) adquirirán más relevancia en este ámbito.

Los recientes ataques de ransomware a nivel mundial, evidencian los riesgos al que se exponen los centros hospitalarios en caso de que estos códigos maliciosos bloqueen o encripten información de sistemas operacionales claves, donde reside toda la información clínica y personal de un paciente, lo cual, puede resultar en una amenaza grave para la continuidad operativa de la organización y la atención oportuna de los pacientes.

De conformidad con lo expuesto, con el fin de reflejar el impacto generado a la prestación de los servicios de Consulta Externa a causa de la desconexión de los sistemas de información institucional, mediante oficio AS-AAS-153-2022 del 20 de julio de 2022, este Órgano de Fiscalización informó a la Gerencia Médica, el resultado de las visitas realizadas a los hospitales: Dr. Rafael A. Calderón Guardia, Dr. Tony Facio Castro, Dr. Maximiliano Peralta Jiménez, San Vicente de Paúl, William Allen Taylor y las Áreas de Salud: La Unión, Carrillo, Moravia, Oreamuno-Pacayas-Tierra Blanca, Heredia -Virilla, Valle la Estrella, indicando entre algunos de los aspectos más relevantes, lo siguiente:

" (…) ***Citas y agendas médicas:***

(…) de las visitas efectuadas a los centros de salud, se comprobó que el Área de Estadísticas en Salud del Nivel Central, remitió el 30 de junio de 2022, un archivo en Excel con la programación de citas médicas correspondientes al periodo de julio a diciembre de 2022; sin embargo, las unidades expusieron que a su criterio ese registro fue remitido de manera "tardía" para el desarrollo oportuno de la gestión y trámites administrativos, como contactar a los usuarios, verificación de agendas (espacios disponibles) futuras programaciones de citas, sustituciones entre otras actividades propias de los funcionarios de REDES para el mes de julio.

(…) un factor crítico en la continuidad de los procesos de consulta externa es la apertura de las agendas médicas, en procura de brindar atención oportuna a los usuarios que requieren mejorar su estado de salud.

Registro de la información de las atenciones médicas (expedientes físicos) en el Expediente Digital Único en Salud (EDUS).

(…) preocupa a este Órgano de Control y Fiscalización, la falta de acceso al historial clínico de los usuarios, por cuanto, los expedientes físicos actualmente se encuentran desactualizados, debido a que el EDUS es el mecanismo que ha dispuesto la CAJA para detallar la clínica de los pacientes, aunado a otros datos relevantes como: Intervenciones médicas, sociales, tratamientos, medicamentos, entre otros registros propios del proceso de atención (…) Además de que podría darse la apertura o duplicidad de expedientes en los centros de salud institucional.

Adicionalmente, no se identificó una estrategia para el resguardo y respaldo de la información física hojas de evolución u otros instrumentos para la anotación de la atención médica brindada, aspecto que representa un riesgo de seguridad, confiabilidad y oportunidad de la información (…)

Es importante mencionar, además, que la institución no ha dispuesto una estrategia, procedimiento o método que permita incluir la información de las atenciones médicas efectuadas desde el 31 de mayo 2022, en el Expediente Digital Único en Salud, así como en otros sistemas de información institucional, debido a la desconexión de los sistemas informáticos, situación que genera incertidumbre a los funcionarios de los centros médicos que deberán efectuar esta tarea (…)

Considerando los volúmenes de datos que se están produciendo y almacenando de forma manual debido a las atenciones médicas que brinda la institución, en citas, tratamientos, historia clínica, procedimientos, egresos, entre otros, es de relevancia responder ágilmente a los cambios del entorno para el desarrollo operacional y estratégico de la CAJA, particularmente en el ambiente de la prestación de los servicios médicos, por lo que disponer de una estrategia tendiente a agilizar la data de información de forma adecuada y sistematizada, contribuirá en la calidad y seguridad de la atención que se brinda a los usuarios.

Otro aspecto a considerar, lo constituyen los riesgos asociados al reproceso, por cuanto realizar las actividades de digitación manual, está vinculado al error involuntario, sobre todo en la eventualidad de incorporación de personal, ya sea mediante contratación de terceros u otro mecanismo de contingencia, que implique la ejecución de estas actividades a través de funcionarios que no dispongan de los conocimientos técnicos - médicos necesarios para el registro y tratamiento adecuado de los datos o información, lo que podría incidir en la veracidad de la historia clínica de los asegurados, aunando a los costos directos e indirectos tales como: mano de obra y tiempo extraordinario.

• Personal de REDES en los centros médicos.

(…) con el ataque cibernético que sufrió la institución, estos funcionarios han debido adaptar su trabajo a las circunstancias actuales, lejos del uso de tecnologías de información y generando la necesidad de laborar en jornadas extraordinarias, aspectos que podrían repercutir en la salud física y mental del personal, así como en la prestación de servicios a los usuarios; además del impacto económico que implica el pago de tiempo extraordinario (…)".

Del oficio anterior, se puede extraer un panorama de algunas de las afectaciones sufridas en centros hospitalarios, origen de la materialización del riesgo de un ciberataque en nuestra institución.

2.2 Recurso Humano:

Los riesgos de seguridad pueden provenir de amenazas externas malintencionadas, así como de infracciones de seguridad internas. Por ejemplo, cuando un empleado abre lo que parece ser un inocente archivo adjunto de correo electrónico y los datos de la organización se ven comprometidos.

Según encuesta realizada por la empresa Kaspersky[1], entre trabajadores del sector de la salud en EE. UU. y Canadá, reveló que aproximadamente un tercio de todos los encuestados (32 %) nunca había recibido capacitación en seguridad cibernética en su lugar de trabajo; asimismo, uno de cada 10 de los colaboradores en puestos directivos también admitió que desconocían la existencia de una política de ciberseguridad en su organización.

La capacitación en seguridad cibernética es muy importante, los trabajadores hospitalarios sin conocimientos tecnológicos académicos pueden aprender a manejar correctamente los archivos adjuntos de correo electrónico, las unidades de memoria flash y los enlaces, además, es importante explicar lo que sucede cuando una determinada tecnología falla y cómo se pueden reconocer esos fallos. Cuando existe un concepto de ciberseguridad bien pensado, con sistemas endurecidos, redes seguras y personal debidamente formado, es más sencillo disminuir los riesgos existentes en la gestión diaria.

En relación con lo anterior, la Caja Costarricense de Seguro Social, según datos del 14 de mayo de 2022, extraídos del Sistema de Información Estadística de Recursos Humanos, disponía (en ese momento) de 62 575 trabajadores (17 957 en propiedad y 44 618 interinos) de los cuales aproximadamente 48 962 (78 %) de los funcionarios carecen de conocimientos técnicos o profesionales en Tecnologías de Información y Comunicaciones, ya que sus puestos o labores se encuentran orientados a los ámbitos de salud o administrativos; lo cual ante la carencia de capacitación en materia de ciberseguridad representa una oportunidad significativa para que los delincuentes cibernéticos, mediante el phishing u otras técnicas de engaño, puedan accesar a las redes y sistemas institucionales, ocasionando situaciones como la suscitada el 31 de mayo del presente año.

Un personal bien informado junto con un programa robusto y automatizado de ciberseguridad y control de amenazas reducirá el impacto de los ciberataques a partir de la prevención y la detección temprana.

2.3 Tendencias de ciberseguridad en organizaciones del sector salud:

Conocer las tendencias en ciberseguridad es una forma de buscar soluciones para hacer entornos más seguros para todos, a nivel internacional, se observa, cada vez más, que centros hospitalarios y organizaciones de atención de la salud, implementan prácticas innovadoras e infraestructura altamente segura para mantener una ventaja en el futuro, ante el creciente aumento de ciberataques.

[1] Kaspersky: empresa de ciberseguridad privada que se fundó en 1997 sobre la base de una colección de módulos antivirus creados por Eugene Kaspersky, un experto en ciberseguridad y CEO desde 2007.

Con el fin de proteger la información de los pacientes y su negocio, es necesario combinar herramientas de seguridad rentables y altamente efectivas con las mejores prácticas de ciberseguridad tanto a nivel de TI como de los empleados.

Las soluciones Zero Trust, seguridad de acceso “Just in time” y la tecnología de nube son algunas de las tendencias en materia de ciberseguridad en el 2022.

Seguridad Zero Trust:

Las organizaciones podrían recurrir a soluciones y marcos de confianza cero para garantizar una visibilidad y un control completos de sus redes a medida que los ciberdelincuentes evolucionen sus tácticas. Cada vez más empresas dedicarán su tiempo a ayudar a entender los motivos de las malas prácticas y cómo pueden protegerse mejor ante un posible ataque.

La seguridad Zero Trust (ZT) proporciona la visibilidad y los controles de seguridad necesarios para proteger, administrar y monitorizar cada dispositivo, usuario, aplicación y red. El modelo de seguridad Zero Trust sigue el principio de control de acceso de menor privilegio donde la identidad del usuario se verifica en tiempo real cada vez que se solicita un recurso.

El acceso con menos privilegios depende de la autenticación multifactor (MFA) o la autenticación de dos factores (como una contraseña y un dispositivo confiable o código temporal). Incluso una vez autenticado, un individuo solo puede acceder a recursos o aplicaciones definidos de forma granular tal como se define en una política de seguridad.

En resumen, Zero Trust comienza con la suposición de que no se puede confiar en todos los conectados hasta que se demuestre lo contrario. Esto hace posible un control mucho más granular y distribuido sobre el acceso seguro a datos confidenciales y recursos internos que el que existía con seguridad basada en el perímetro o con controles de seguridad física.

Los beneficios de Zero Trust significan que ha ganado una amplia aceptación y adopción, con compañías como Google adoptando una forma de Zero Trust llamada BeyondCorp que asume que la red interna es tan peligrosa como Internet.

La meta es llegar a la confianza cero de cualquier elemento de la red hasta que es verificado.

Seguridad de acceso “Just in time”:

La seguridad de accesos Just-In-Time (JIT) es una práctica fundamental que ayuda a reducir los privilegios de acceso excesivos, concede a los usuarios, procesos, aplicaciones y sistemas derechos y accesos determinados para realizar ciertas tareas definidas durante un periodo de tiempo preestablecido.

La seguridad Just-In-Time, como política, tiene por objetivo minimizar el riesgo de los privilegios permanentes para limitar la exposición a potenciales ciberataques. Cuando muchos usuarios de una organización disponen de una gran cantidad de privilegios en todo momento, las posibilidades de sufrir un robo, explotación y escalada de credenciales para robar secretos, cifrar datos o detener sistemas aumenta exponencialmente.

Al conceder privilegios elevados únicamente cuando es necesario, se consigue limitar al mínimo la exposición y, además, permite a los usuarios continuar con su trabajo.

El informe de vulnerabilidades de Microsoft de 2021 afirma que el año pasado la elevación de privilegios fue la categoría de vulnerabilidad número uno, un 44% del total, lo que supone un aumento de casi el doble con respecto a 2020.

El objetivo del JIT es asignar automáticamente los privilegios que un usuario necesita sobre la marcha y abordando los tres principales factores de acceso: ubicación, tiempo y acciones.

- ¿Desde qué lugar pretende acceder un usuario?
- ¿Durante cuánto tiempo necesitará tener acceso?
- ¿Está autorizado a trabajar durante dicho periodo de tiempo?
- ¿Qué es lo que pretende hacer exactamente con ese acceso?

Las políticas de seguridad Just-In-Time (JIT) ayudan a las empresas a:

- Mejorar su postura de ciberseguridad general.
- Eliminar privilegios excesivos e implementar la política de Zero Standing Privileges.
- Optimizar y automatizar los procesos de escalada de privilegios.
- Gestionar usuarios privilegiados que sean tanto máquinas como humanos.
- Habilitar los accesos remotos seguros a los activos sensibles.
- Facilitar la seguridad sin afectar a la productividad.

La tecnología de la nube:

Las organizaciones de atención de salud deben transformarse digitalmente para cumplir con las expectativas y estándares modernos, la adopción de la tecnología de nube podría ser una de las opciones para dicha transformación. Elegir la solución correcta garantiza que las organizaciones de salud colaboren para obtener mejores resultados, optimicen las operaciones y protejan la información altamente confidencial.

Dicha tecnología, puede garantizar que los datos de los pacientes estén disponibles con conectividad continua y continuidad del negocio, además, proporcionará acceso oportuno y confiable a la información para la toma de decisiones (basada en datos) y proteger los servicios operativos en caso de una interrupción.

La tecnología de nube correcta permite a las organizaciones:

- **Proteger** eficazmente la infraestructura, los datos y las aplicaciones de las ciberamenazas cada vez más sofisticadas.
- **Acceder fácilmente** a los datos de salud.
- **Mantenerse** seguro y conforme a las normas.
- **Mantener** el control sobre quién puede acceder a los datos confidenciales.
- **Equilibrar** la seguridad de los datos con permisos controlados.
- **Ser** transparente en sus procesos de negocio.
- **Proteger** la integridad de los datos y garantizar que nunca se compartan ni se vendan.
- **Asegurarse** de que sus sistemas y datos estén siempre disponibles para evitar interrupciones en los servicios.
- **Actualizar** a tecnologías y soluciones digitales modernas para expandir su organización mientras detecta, contiene y repara posibles vulnerabilidades.

Además, a través de la tecnología de la nube los centros de atención de salud pueden implementar avances, tales como:

- Mejorar la interacción con el paciente.
- Potenciar la colaboración entre los equipos de salud.
- Mejorar la información clínica y operativa.
- Proteger la información de salud.

En la atención de salud, cada nuevo avance genera una significativa cantidad de datos altamente confidenciales, lo cual significa más requisitos de almacenamiento, mayores obligaciones legales y costos más altos.

Con un enfoque optimizado, esta tecnología podría aumentar la transparencia y controlar el flujo de datos tanto para el cuidado personalizado como para los procesos de salud de precisión, lo que facilita el seguimiento y el control de datos confidenciales entre dispositivos y aplicaciones.

2.4 Atenciones médicas hospitalarias en la Caja Costarricense de Seguro Social

Según datos extraídos de la Memoria Institucional 2021 de la CCSS, durante ya hace muchas décadas la Caja Costarricense de Seguro Social ha venido aportando y evolucionando con recursos TIC a lo largo y ancho de toda la organización, siempre buscando beneficios para la población que atiende los servicios de salud y la eficiencia de los procesos partir de la participación de la infraestructura social interna.

Además, del citado documento es importante señalar que, específicamente en el área de hospitalización por región y establecimiento de salud. En el año 2021, se atendió un total de 296 186 egresos hospitalarios, lo que representó un aumento de 33 045 egresos respecto al 2020. Cabe rescatar que los indicadores para estos años están influenciados por los efectos de la pandemia y la reconversión de los servicios de salud para atender la emergencia.

Asimismo, el índice de ocupación hospitalaria alcanzó el 70% a nivel del país, un valor similar al recomendado internacionalmente. Considerando que la reconversión de camas en preparación a la atención de los pacientes afectados por el COVID-19, implicó una disminución en la oferta en comparación con años anteriores a la pandemia, esto para la liberación de los recursos requeridos, lo cual repercute en un descenso del índice
de ocupación.

2.4.1 Atención de emergencias/urgencias

En el 2021 se realizaron casi 5 millones de atenciones en los servicios de emergencias/urgencias, aproximadamente el 62,7 % (9 621 925) de atenciones de urgencias se realizaron en las áreas de salud; no obstante, el 37,3 % (1 864 996) se efectuaron en los hospitales y posiblemente corresponden a los casos de mayor gravedad.

2.4.2 Servicios de apoyo

a) Farmacia

Del total de recetas despachadas durante el 2021, el 69% se prescribieron en consulta externa, 8% en el servicio de urgencias y un 8% en hospitalización, el 15% restante corresponde a otras áreas de atención, así como servicios internos y alternativos. Con respecto al año anterior, en el servicio de hospitalización para ese año se da un aumento del 65% con respecto al año anterior (4,4 millones de recetas despachadas). A nivel nacional se entregaron 23,2 medicamentos en promedio por paciente hospitalizado, lo que representa un aumento con respecto al año anterior, ya que se registraba un valor de 14,5 medicamentos emitidos por egreso. La región Brunca representaba la mayor razón el año anterior y, para el 2021, este lugar lo toman los hospitales nacionales y los centros especializados con un promedio de 31 medicamentos emitidos por cada egreso.

b) Laboratorio

En los servicios de hospitalización a nivel nacional, durante el 2021, se realizó en promedio 39,9 exámenes por paciente hospitalizado (mientras que en el 2020 fue de 35,8 y en el 2019 de 25,9). Es decir, se presenta una tendencia creciente, siendo el último aumento respecto al año anterior de 4 exámenes por paciente. Los hospitales nacionales y centros especializados presentan la mayor razón con 66 exámenes realizados por egreso hospitalario, seguido por la región Chorotega con una razón de 37,7.

c) Estudios de radiología e imágenes médicas

Para el año 2021 se hicieron aproximadamente 1,68 millones de estudios radiológicos en los establecimientos de salud de todo el país, los cuales requirieron aproximadamente 1,82 millones de placas; es decir una razón de 1,08 placas por estudio. Respecto al 2020 se presenta un aumento de 394 mil estudios y de 331 mil placas. Si comparamos las razones del 2019 al 2021 son de: 1,27; 1,16 y este año de 1,08; así que presenta una tendencia decreciente del uso de placas por estudio. Esta disminución se debe al esfuerzo institucional en digitalizar este servicio, significando una economía para la institución, una atención más oportuna al paciente y principalmente una reducción en la contaminación con los materiales utilizados, contribuyendo de esta manera en disminuir la huella de carbono

De la información anteriormente expuesta, se observa que institucionalmente los centros hospitalarios generan un importante porcentaje de las atenciones médicas, recetas de medicamentos, exámenes de laboratorio y estudios de radiología e imágenes médicas en los servicios de salud, lo cual, representa una cantidad importe de registros o datos digitales (almacenados en bases de datos), siendo relevante el fortalecimiento de las medidas de ciberseguridad y la implementación de tecnologías innovadoras, con el fin de garantizar de manera razonable la protección de la información clínica y confidencial de los pacientes, así como la continuidad del negocio ante cualquier irrupción.

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 XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, 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 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".*

Según el marco referencial COBIT 5 (Objetivos de Control para las Tecnologías de Información), en la descripción del proceso DSS04, DSS04.02 y DSS04.04 se indica lo siguiente:

> *"establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa".*

"evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción".

"probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera".

III. CONSIDERACIONES

La institución requiere adoptar medidas estratégicas y estructurales para proteger el entorno hospitalario de ciberataques, ya que una interrupción de las tecnologías y los equipos médicos (digitalizados) puede resultar en una amenaza grave para la continuidad operativa de la organización y la atención oportuna y de calidad de los pacientes.

La ciberseguridad hospitalaria es un objetivo que se mueve rápidamente, las amenazas y vulnerabilidades son abundantes con la adopción y el uso de nuevas tecnologías y aplicaciones. Es vital gestionar de forma adecuada la seguridad de la información en salud, ya que es un elemento esencial que supone la implementación de diversas medidas organizativas y técnicas que deben ser abordadas desde diferentes ámbitos: legal, normativo, tecnológico y educativo, entre otros.

Los constantes ciberataques efectuados en el sector salud y centros médicos, a nivel mundial, no deben ser un elemento que frene el imparable y necesario proceso de digitalización hospitalaria, al contrario, la mejor manera de controlar y proteger la información de los pacientes y las infraestructuras críticas es con el uso de herramientas y tecnologías existentes que permiten controlar accesos no permitidos, bloquear virus y ataques varios, registrar cada uno de los acceso a información protegida y controlar otras vulnerabilidades de la evolución tecnológica.

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 y la gestión de Tecnologías de Información y Comunicaciones en los centros hospitalarios.

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: 2022.08.17 21:11:24 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AEBB/lbc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General-1100.
Auditoría.