CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821
Correo electrónico: coinccss@ccss.sa.cr

Al contestar refiérase a: **ID-122250**

AS-ATIC-0107-2024
26 de agosto de 2024

Doctor
Roberto Aguilar Tassara, director médico

Máster
Marlon Méndez Torres, director financiero administrativo

Ingeniero
José Luis Porras Barquero, jefe
Centro de Gestión Informática
CENTRO NACIONAL DE REHABILITACIÓN HUMBERTO ARAYA ROJAS – 2203

Estimados Señores:

ASUNTO:	**Oficio de Asesoría referente a las condiciones actuales de las tecnologías de información y comunicaciones del Centro Nacional de Rehabilitación Humberto Araya Rojas.**

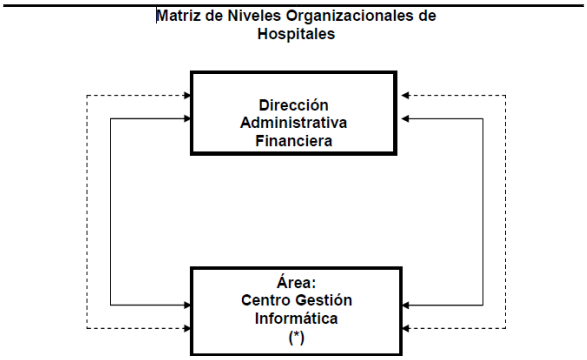
En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2024 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, se procede a asesorar sobre las condiciones actuales de las tecnologías de información y comunicaciones en el Centro Nacional de Rehabilitación Humberto Araya Rojas, con la finalidad de informar os riesgos en temas tales como: condiciones de seguridad física del Centro de Gestión Informática, gabinetes de comunicaciones y centro de datos, control de equipos TIC y bodega de almacenamiento, así como el estado actual del Plan de Continuidad de la Gestión de Tecnologías de Información. En ese contexto, se exponen los siguientes elementos para su consideración.

I. ANTECEDENTES

El Centro Nacional de Rehabilitación Humberto Araya Rojas, dispone de un Centro de Gestión Informática (CGI), cuya estructura orgánica y funcional se encuentra establecida en el Modelo de Organización de los CGI (octubre 2013), mismo cuyas modificaciones fueron aprobadas por la Junta Directiva en el artículo No. 44 de la sesión No. 8555 del 26 de enero de 2012 y artículo No. 32 de la sesión No. 8658 del 29 de agosto de 2013.

De acuerdo con dicho modelo de organización, los CGI Tipo B son responsables de velar por el adecuado funcionamiento de las Tecnologías de Información y Comunicaciones en los niveles gerenciales, regionales, y locales, correspondiente este último a unidades como hospitales (nacionales, especializados, regionales y periféricos), áreas de salud, y sucursales. El CGI del hospital objeto de la presente evaluación corresponde al Tipo B, y su nivel organizacional se muestra seguidamente:

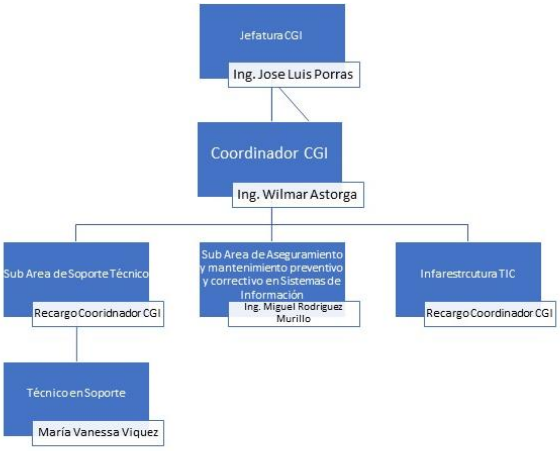
Figura 1
Matriz de Nivel Organizacional
Centro de Gestión Informática Hospitales
Tipo B
2013



Fuente: Modelo de Organización de Centros de Gestión Informática, CCSS, 2013

De conformidad con información suministrada por el Ing. José Luis Porras Barquero, jefe del CGI del centro médico, actualmente dispone de 4 funcionarios, organizados de la siguiente manera:

Figura 2
Organigrama
Centro de Gestión Informática
Centro Nacional de Rehabilitación
2024



Fuente: Centro de Gestión Informática, Centro Nacional de Rehabilitación, 2024

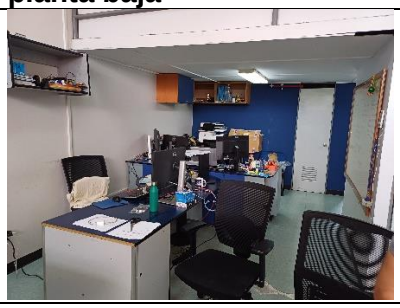
II. Sobre la gestión de Tecnologías de Información y Comunicaciones.

Mediante visita efectuada al Centro Nacional de Rehabilitación el 8 de agosto de 2024, se procedió a la verificación de la gestión de las tecnologías de información y comunicaciones en aspectos tales como seguridad física de las instalaciones del CGI y gabinetes de comunicaciones, control de acceso de visitantes, inventario de activos, plan de continuidad, control de bodega de repuestos, entre otros, de lo cual se evidenció oportunidades de mejora que se detallan seguidamente.

- **Condiciones de seguridad física del CGI**

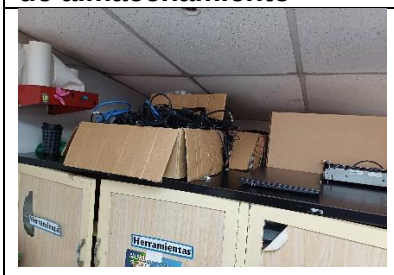
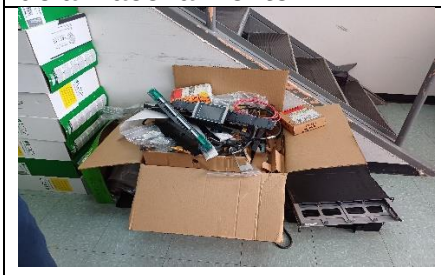
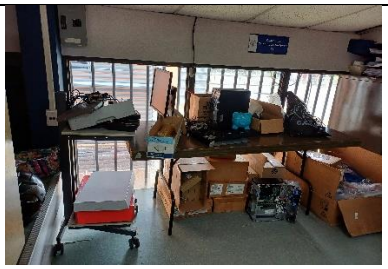
El Centro de Gestión Informática está ubicado en una zona externa del centro médico, contiguo a instalaciones de ingeniería y mantenimiento, está constituido por una primera planta en la cual se tiene una mesa de usos múltiples (comedor, reuniones) y dos escritorios usados por el Ing. Porras Barquero y Astorga Granados y una segunda planta en donde se ubican los funcionarios de soporte y mantenimiento de equipo, según se observa en las siguientes imágenes:

Estado
Centro de Gestión Informática
Centro Nacional de Rehabilitación
2024

Fotografía 1: Mesa uso variado	**Fotografía 2: Escritorios planta baja**	**Fotografía 3: Escritorio Planta Alta**
		

Aunado a lo anterior, se evidenciaron múltiples espacios usados para almacenamiento de equipos, cables, repuestos y otros elementos, los cuales están desordenados y carecen de un inventario que permita determinar aspectos como cantidad, estado, uso, entre otros.

Áreas de Almacenamiento
Centro de Gestión Informática
Centro Nacional de Rehabilitación
2024

Fotografía 4: Múltiples áreas de almacenamiento	**Fotografía 5: Múltiples áreas de almacenamiento**	**Fotografía 6: Múltiples áreas de almacenamiento**
		
Fotografía 7: Múltiples áreas de almacenamiento	**Fotografía 8: Múltiples áreas de almacenamiento**	**Fotografía 9: Múltiples áreas de almacenamiento**
		

En relación con el acceso el CGI dispone de una puerta de vidrio con visibilidad desde el interior de los funcionarios o visitantes que requieren ingresar, no obstante, carece de mecanismo de control de accesos electrónicos, biométricos, o de una bitácora que permitan identificar quienes ingresan y la gestión que realizan.

Al respecto el Ing. Porras Barquero, indicó:

> *"Se está trabajando en un proyecto que involucra todo el hospital para dotarlo de accesos biométricos, el proyecto lo está desarrollando el servicio de aseo y vigilancia. El proyecto se denomina de seguridad electrónica, en este momento el proyecto está en consulta con la Dirección de Servicios Institucionales, quienes aún no resuelven sobre la viabilidad del mismo.*
>
> *Este proyecto incluye los elementos de seguridad como CCTV, controles de accesos electrónicos, agujas de parqueos y sensores perimetrales, para todo el centro médico."*

En ese sentido, las condiciones descritas podrían provocar una afectación a los recursos institucionales almacenados en el Centro de Gestión Informática, al desconocer la cantidad, estado, uso de los múltiples elementos ubicados en las cajas y espacios identificados, aunado a lo anterior, la carencia de mecanismos de control de acceso y de visitantes eventualmente incrementaría el riesgo de eventuales sustracciones o perdidas de materiales, repuestos o otros activos.

- **Condiciones de seguridad de gabinetes de comunicación y Centro de datos.**

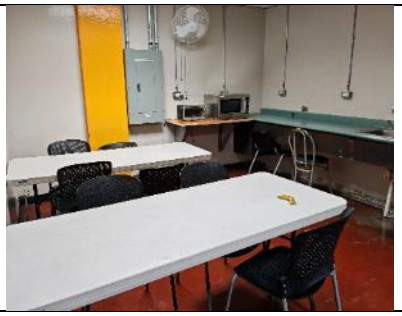
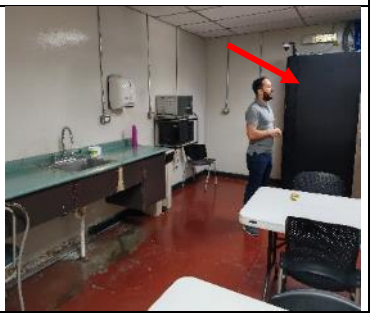
Mediante recorrido realizado el 8 de agosto del 2024, en las instalaciones del Centro Nacional de Rehabilitación en compañía de los funcionarios Ing. José Luis Porras Barquero, jefe e Ing. Wilmar Arturo Astorga, analista de sistemas, ambos del Centro de Gestión Informática de ese centro médico se evidenciaron oportunidades de mejora en las condiciones de seguridad física de los gabinetes de comunicación y centro de datos, esencialmente relacionadas con la protección de los mismos ante intentos de acceso por parte de pacientes o visitantes del hospital, además de la ubicación de un gabinete en una zona de alimentación del personal y asegurados.

Se debe indicar que todos los gabinetes de comunicaciones están dotados de mecanismos de cerradura electrónica que se activan mediante lectura de huella digital o código numérico, además, disponen de cámara de vigilancia, climatización interna, UPS incorporado y sistema de notificación de acceso (mediante correo electrónico automático).

Además, es necesario señalar que cada gabinete de comunicaciones dispone de una cámara de vigilancia ubicada en la parte superior que permitiría monitorear sus puertas de acceso, no obstante, al momento de la visita, las mismas se encuentran fuera de funcionamiento. En ese sentido, su puesta en funcionamiento eventualmente disminuiría los riesgos relacionados con accesos no autorizados, considerando además que algunos de ellos se ubican en espacios de alto tránsito de pacientes, como se detalla seguidamente.

En ese contexto, se evidenció la ubicación de un gabinete en el comedor auxiliar, instalaciones que permiten a funcionarios y visitantes el consumo de alimentos y está dotado de hornos de microondas, fregaderos y tuberías de agua potable y servida, cercanos al gabinete como se muestra en las siguientes imágenes:

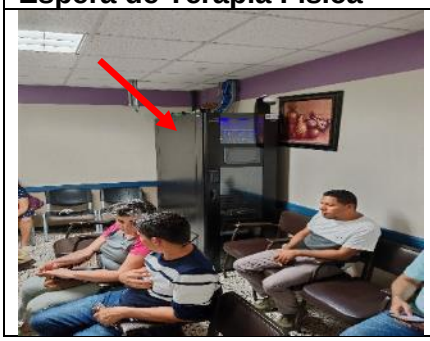
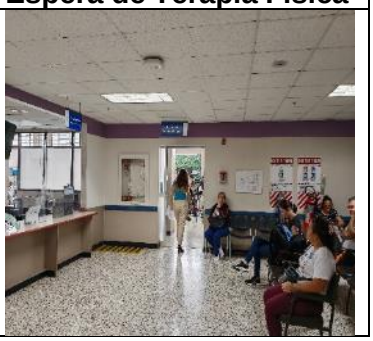
Gabinetes de Comunicaciones
Centro Nacional de Rehabilitación
2024

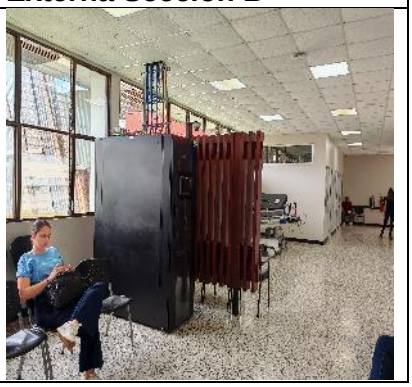
Fotografía 10: Comedor Auxiliar	**Fotografía 11: Comedor Auxiliar**	**Fotografía 12: Comedor Auxiliar**
		

Fotografía 13: Comedor Auxiliar


Aunado a lo anterior, al menos tres gabinetes están ubicados en las salas de espera de Terapia Física y consulta externa A y B, los cuales carecen de mecanismos de seguridad que restrinjan el acceso de terceros al perímetro a los mismos. Según se muestra en las siguientes imágenes:

Gabinetes de Comunicaciones
Centro Nacional de Rehabilitación
2024

Fotografía 14: Sala de Espera de Terapia Física	Fotografía 14: Sala de Espera de Terapia Física	Fotografía 16: Sala de Espera de Terapia Física
		

Fotografía 17: Consulta Externa Sección B	**Fotografía 18: Consulta Externa Sección B**
	

Fotografía 19: Consulta Externa Sección A	**Fotografía 20: Consulta Externa Sección B**
	

Respecto a los restantes gabinetes se ubican en áreas de acceso controlado tales como: farmacia y salas de hospitalización entre otros, por lo que se minimiza el riesgo de accesos no autorizados.

En relación con el centro de datos, está ubicado en el área administrativa del centro médico, dispone de una puerta de acero con cerradura electrónica, carece de una bitácora de acceso y se observan rociadores de agua en su interior. Los gabinetes ubicados en su interior disponen, de mecanismos de control de acceso mediante cerradura electrónica que se activa mediante código numérico o lectura de huella digital, además, cámara de vigilancia (no se encuentra funcionando), climatización, UPS incorporado y sistema de notificación de acceso (por medio de correo electrónico).

En ese contexto, la ubicación de gabinetes de comunicación en espacios de alto tránsito de pacientes y familiares expone estos elementos a riesgos tales como: accesos no autorizados, apertura de puertas o vandalismo, ciertamente la administración del centro médico ha instalado gabinetes con estándares y mecanismos de seguridad como apertura con huella digital, paneles de metal, entre otros; no ha implementado la utilización de las cámaras de vigilancia integradas en los mismos. Aunado a lo anterior, un gabinete se ubica en un espacio utilizado para alimentación de visitantes y personal de centro médico, lo que eventualmente podría afectar el equipo de comunicaciones al contar en esa ubicación con microondas, fregaderos y tuberías.

- **Sobre el control de equipos de TIC.**

Esta Auditoria procedió a la verificación de 30 activos incluidos en el inventario proporcionado por el Centro de Gestión Informática del Centro Nacional de Rehabilitación Humberto Araya Rojas, determinándose que los equipos placas 788667 y 788669 no fueron localizados al momento de efectuar la prueba descrita.

Es necesario indicar que corresponden a servidores de mediana y baja complejidad respectivamente, los cuales están en uso, según consulta realizada al Sistema Contable de Bienes Muebles[1]. Sobre este particular, es necesario que la Administración del Centro informe a este Órgano de Fiscalización.

Sobre la bodega de almacenamiento de activos y repuestos del CGI

En la visita efectuada al Centro de Gestión Informática, se evidenció la existencia de una bodega de almacenamiento de activos y repuestos usados en las labores propias de esa unidad, no obstante, carece de inventario actualizado que permitan determinar los productos, repuestos o activos almacenados, su cantidad, estado y costo. Aunado a lo anterior, la puerta de acceso se encontraba cerrada, sin embargo, la llave estaba puesta en el llavín de acceso.

Las condiciones de almacenamiento se muestran seguidamente:

Bodega
Centro de Gestión Informática
Centro Nacional de Rehabilitación
2024

Fotografía 21: Bodega de Almacenamiento	**Fotografía 22: Bodega de Almacenamiento**	**Fotografía 23: Bodega de Almacenamiento**
		

Al respecto el Ing. Porras Barquero indicó que no se han efectuado inventarios en la bodega desde su apertura, hace aproximadamente tres años.

En ese contexto, la carencia de controles de repuestos y activos u otros elementos almacenados en la bodega del centro de gestión informática, facilitaría eventuales perdidas o sustracciones, al desconocer aspectos como: cantidad, estado, uso. Aunado a lo anterior, es necesario señalar una posible afectación a los recursos institucionales, al no tener claridad de las cantidades resguardadas, impactando en posteriores procesos de adquisición, dado que se solicitarían cantidades menores o mayores a las requeridas.

[1] Consulta realizada al SCBM el 16 de agosto del 2024.

- **Sobre el Plan de Continuidad de la Gestión**

Se evidenció que el Centro Nacional de Rehabilitación, dispone de un "Plan de Continuidad de la Gestión de Tecnologías de Información y Comunicaciones, no obstante, la versión más reciente corresponde al año 2020 (versión 3.5), lo que resulta relevante considerando los diversos cambios en la infraestructura tecnológica que ha experimentado el centro médico, así como los diversos eventos que ha enfrentado la institución en ese periodo.

Aunado a lo anterior, la información contenido en el mencionado plan presenta una evidente obsolescencia, tal como la inclusión de servidores con sistema operativo Windows Server r2 cuyo soporte venció el 10 de octubre de 2023.

Al respecto el Ing. Porras Barquero, indicó que fue convocado por la Dirección de Tecnologías de Información y Comunicaciones a un proceso de capacitación sobre las nuevas plantillas y metodología para el desarrollo del Plan de Continuidad.
En ese sentido, la actualización del plan de continuidad de la gestión TIC, permitiría a la administración una mejor respuesta ante la materialización de los riesgos identificados.

III. Consideraciones normativas

Las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información, emitidas por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones, en su apartado IV. Gestión de los Riesgos Tecnológicos, señala:

"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que este integrada al sistema especifico de valoración del riesgo institucional y considerando el Marco de gestión de TI que le resulte aplicable.

La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."

Las Normas mencionadas en su apartado IX "Seguridad y Ciberseguridad" señala:

> *"(…) 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 (…)."*

Las Políticas Institucionales de Seguridad Informática en su artículo 10.11. PSI-UAR-011 Administración del espacio físico en los centros de cómputo, establece:

"(…) Los equipos en los cuales se almacenan y procesan datos críticos que colaboran con el cumplimiento de los servicios informáticos, deben estar ubicados en un espacio especial que cumpla con condiciones básicas de seguridad para la protección de los datos que contienen y del equipo en sí. Dichas condiciones entre otras son: protección contra humedad y/o polvo, espacio solo accesible por los administradores, uso de cables de corriente alterna debidamente aterrizados, uso de aire acondicionado (…)".

La Guía de Mejores Prácticas en la Gestión de los Centros de Producción de Datos DTI-I-SI-0003, establece lo siguiente:

"Se realizó una adaptación del estándar internacional TIA 942 para establecer los requerimientos mínimos que debe contemplar un centro de producción de datos para la CCSS, para esto se dividió en 3 de niveles de complejidad los centros de producción de datos en la Institución: Baja, mediana y alta complejidad como se detalla a continuación:

Centros de Producción de datos, Mediana Complejidad, CGI Gerenciales - Hospitales Nacionales y Especializados -Sucursales

(…) ***Seguridad Perimetral:*** *Registro en bitácora con aval de un funcionario informático local (…)*

Cámaras de vigilancia: *Cámaras con grabación por movimiento, con almacenamiento local y respaldo remoto (...)*

Control de acceso electrónico: *Acceso mediante tarjeta de proximidad (…)*

Acceso de Terceros: *El tercero, siempre debe de hacerse acompañar de un local, con el objetivo de que monitoree todas las actividades desarrolladas. - Debe de realizarse el registro de ingreso y egreso en bitácora - Nunca debe tomar videos o fotografías de las instalaciones, equipos, configuraciones, otros (…)*

Puertas: *- Dimensiones que permitan el paso de los equipos. - Construidas con material retardante al fuego - Cierre electrónico con apertura por tarjeta de proximidad o biométrico (valorando que el nivel de efectividad sea superior a un 80%) (...)*

Condiciones Ambientales: *- Aire acondicionado acorde a las recomendaciones del fabricante y la carga total de recursos en sitio (...)*

Mecanismo de extinción de fuego*: - Aplicar productos no líquidos, químicos que no sean corrosivos a los equipos. - Paredes y pintura retardante de fuego - A nivel de canalizaciones los materiales aislantes deben ser incombustibles y que no desprendan polvo - Los detectores de humo y de calor se deben instalar en el centro de producción y en todas las áreas anexas - Deben estar cubiertos por el sistema de alarmas local (…)".*

Las Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002, Versión 1.0 abril 2008, apartado 7.11 Norma Para la Política de Administración Espacio Físico en los Centros de cómputo. mencionan al respecto:

De manera muy general, la guía antes mencionada indica que tener controlado el ambiente y acceso físico de los centros de cómputo permite:

- *Disminuir el impacto de siniestros*
- *Trabajar mejor teniendo la sensación de seguridad*
- *Descartar falsas hipótesis si se produjeran incidentes*
- *Tener los medios para luchar contra incidentes*

Adicionalmente en la guía, se indica que, para una instalación y administración adecuadas de los equipos de cómputo administrados por los diferentes Centros de Gestión Informática, deben considerar aspectos que afectan la seguridad física, entre los cuales están los factores humanos y los ambientales. Para controlar los factores ambientales se deben tomar medidas como: clasificar las instalaciones según su nivel de riesgo, la ubicación física correcta y segura de los equipos, así como factores que debe cumplir el centro de cómputo como aire acondicionado, ductos, cableado estructurado, así como mecanismos para protección contra el fuego y por último controles de acceso físico como, registros de firmas, cámaras y alarmas.

Respecto a la vigencia del Plan de Continuidad, las Normas Institucionales en Tecnologías de Información y Comunicaciones en el punto 1.5 “Continuidad de los Servicios de Tecnologías de Información” establece:

> “*Toda unidad de trabajo debe garantizar una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios internos y externos. Para ello se deben elaborar, actualizar, divulgar y aprobar en los niveles correspondientes el plan de continuidad en las unidades de trabajo que utilicen para su funcionamiento TI. Estos planes deben estar documentados, aprobados por la autoridad correspondiente y puestos a prueba, todo ello, según lo dispuesto en Guía para Elaborar Planes de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones emitido por la Subárea de Continuidad de la gestión TIC”.*

Además, el Manual para Elaborar Planes de Continuidad en TIC, en el apartado “Frecuencia de Ensayos” indica:

> *“Los ensayos deben ser realizados al menos una vez al año, o en su defecto de los cambios en el ambiente en las operaciones. No obstante, dependiendo del riesgo, es conveniente elaborar un calendario de ensayos más frecuente y riguroso. Es conveniente tener en cuenta que los resultados de los ensayos deben ser formalmente reportados. Además, en caso de que sea necesario, el Plan podría requerir ser actualizado, para lo cual el CPC debe actualizar un formulario “Mantenimiento del Plan” (PTC014) incluido en esta guía”.*

IV. Consideraciones Finales

En consonancia con lo descrito, la gestión de las tecnologías de información y comunicaciones en el Centro Nacional de Rehabilitación presenta oportunidades de mejora en aspectos relacionados con inventario de equipos, control de repuestos y equipos almacenados en la bodega del servicio, actualización del Plan de Continuidad, condiciones de seguridad del CGI y de gabinetes de comunicaciones, cuyas condiciones actuales podrían afectar los servicios prestados tanto a los clientes internos (usuarios de la plataforma y servicios TIC del centro médico) como a los asegurados.

La situación descrita, en relación con los gabinetes de comunicaciones ubicados en salas de espera, así como en el comedor auxiliar, ciertamente disponen de mecanismos de acceso biométricos y electrónicos, están expuestos a condiciones en las cuales podrían ser vandalizados o afectados por la naturaleza del uso de esas áreas, en las cuales transita de manera irrestricta funcionarios ajenos al CGI y pacientes y familiares que asisten al centro médico. Aunado a lo anterior, la obsolescencia evidencia en el Plan de Continuidad permite establecer que las acciones de recuperación ante lo descrito anteriormente podrían ser insuficientes.

En otro orden de ideas, es necesario indicar que las condiciones evidenciadas en la bodega y en el CGI respecto a los diversos espacios de almacenamiento en aspectos como orden, identificación de elementos almacenados, inventarios, estados de los repuestos o activos, entre otras, podría resultar en un inadecuado manejo de recursos dado que no es posible determinar con claridad todo lo que se tiene y su costo. Esta situación eventualmente facilitaría sustracciones o perdidas de los materiales resguardados.

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, en la gestión de las tecnologías de información y comunicaciones de ese centro médico.

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.08.28 16:24:57 -06'00'

M. S.c. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AAM/ams.

C. Auditoría

Referencia: ID-122250