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

AS-AAO-121-2022
30 de junio de 2022

Doctor
Randall Álvarez Juárez, gerente
GERENCIA MÉDICA - 2901

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

Estimados señores:

ASUNTO: Oficio de asesoría referente a la afectación en los servicios de ingeniería y mantenimiento producto del ataque cibernético del 31 de mayo de 2022.

La Auditoría Interna con fundamento en el Plan Anual Operativo 2022 del Área Auditoría Operacional y con el objetivo de cumplir con las funciones preventivas y de asesoría en relación con las actividades sustantivas desarrolladas en los servicios de Ingeniería y Mantenimiento, aplicó la encuesta denominada: "*Cuestionario relacionado con la afectación producto del ataque cibernético del 31 de mayo de 2022*", con la finalidad de documentar aspectos de interés en la gestión de mantenimiento institucional.

El citado cuestionario dispuso de la participación de 41 centros de salud, que incluyó a los jefes de los Servicios de Ingeniería y Mantenimiento de hospitales Nacionales, Regionales y Periféricos (26 Unidades participantes), jefes de las Áreas Regionales de Ingeniería y Mantenimiento (4 Unidades participantes), jefes de Mantenimiento de Centros Especializados (1 Unidad participó) y 10 jefes de Mantenimiento de Áreas de Salud.

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 la institución a desconectar los sistemas informáticos, a fin de determinar el nivel de afectación. Producto de lo anterior, se inhabilitó el Sistema de Operación, Control y Mantenimiento (SOCO), afectando los procesos sustantivos que realizan los Servicios de Ingeniería y Mantenimiento.

Mediante el oficio GIT-DMI-0448-2022 del 6 de junio de 2022, el Ing. Ronald Ávila Jiménez, director Mantenimiento Institucional, comunicó a las unidades que conforman la Institución, lo siguiente:

> *"…a continuación, encontrará recomendaciones para mantener la gestión de los servicios de mantenimiento a nivel local:*
>
> *1) Se recomienda que las solicitudes de mantenimiento sean gestionadas vía telefónica o por medio de órdenes de servicios físicas, con el objeto de acatar las directrices actuales acerca de la restricción en el uso de la red de comunicación institucional.*
> *2) El servicio de Ingeniería y Mantenimiento o los funcionarios responsables informarán en cada unidad usuaria sobre la forma en la que gestionará las solicitudes de mantenimiento (Vía telefónica u orden de servicio física), para lo cual deberá comunicar el número de teléfono asignado, en caso de ser por llamada, o facilitará a las unidades usuarias por los medios disponibles el formulario para realizar las solicitudes de mantenimiento.*

3) Llevar un registro manual de las solicitudes de mantenimiento recibidas vía telefónica, el cual debe indicar: número de orden, fecha del recibido de la solicitud, nombre del servicio o edificio, nombre del subservicio o número de piso, descripción de trabajo (dado por el solicitante), nombre de funcionario solicitante, número de teléfono o extensión del solicitante, número de activo (De ser necesario), nombre del personal asignado al trabajo, y observaciones. En el caso de que la unidad solicitante no cuente en ese momento con el número de activo, este dato será tomado por el técnico asignado al momento de revisar el equipo.
4) Coordinar con proveeduría la entrega de materiales por medio de solicitudes de material provisionales.
5) Una vez restablecido el funcionamiento del SOCO, cada unidad local de Ingeniería y Mantenimiento deberá elaborar las solicitudes de mantenimiento correspondientes a todos los trabajos que se realizaron mientras el SOCO se encontraba fuera de servicio, con el objeto de registrar en el sistema estos trabajos, así como costos de mano de obra, materiales, entre otros.

Adicionalmente, se adjuntan a manera de referencia formularios "Orden de Servicio Provisional", "Control Registro de Solicitudes de Mantenimiento" y "Salida de Material Provisional", los cuales pueden ser utilizados en la implementación de las recomendaciones de los puntos 2, 3 y 4. En caso de contar con equipo de cómputo e impresora que no estén conectada a la red institucional se podrían imprimir, caso contrario sería utilizar los formatos recomendados, pero de manera manual…".

A continuación, se detallan los principales resultados obtenidos:

II. GRADO DE AFECTACIÓN Y PRINCIPALES ASPECTOS PERJUDICADOS EN LOS SERVICIOS DE INGENIERÍA Y MANTENIMIENTO

Producto de las respuestas recibidas, el 58% de los participantes manifestó que la afectación en la gestión de mantenimiento ha sido moderada, el 26% severa y el 16% leve.

En relación con los principales aspectos perjudicados producto del ataque cibernético, mencionaron los siguientes:

- Ejecución contractual: 53%
- Atención de solicitudes de mantenimiento (SOCO): 77%
- Gestión administrativa (permisos, vacaciones, incapacidades, horas extras, nombramientos, entre otros): 74%
- Desarrollo de proyectos: 60%
- Gestión del mantenimiento (producción, planificación, control, presupuesto): 70%
- Gestión de compras (tramitación de facturas de pago a proveedores, elaboración de carteles, entre otros): 79%
- Herramientas tecnológicas (computadoras, teléfonos, office, Microsoft Teams): 88%
- Mantenimiento preventivo propio: 26%

De lo anterior, se puede señalar que aproximadamente el 26% de las unidades participantes, mencionaron que la afectación en las labores sustantivas del servicio ha sido severa, además, los principales aspectos perjudicados han sido en la gestión de compras, suspensión del uso de herramientas tecnológicas, atención de solicitudes de mantenimiento a través del SOCO y la gestión administrativa.

III. SOBRE LA INFORMACIÓN Y COMUNICACIÓN RECIBIDA DEL NIVEL CENTRAL, REGIONAL Y LOCAL

En relación con las directrices emitidas por la Gerencia de Infraestructura y sus dependencias, el 77% mencionó que ha recibido información para la atención de los procesos sustantivos de mantenimiento y el 23% consideró que no ha recibido información. Sobre la calidad de esa información, el 51% refiere que es deficiente, el 16% clara y concisa, el 14% suficiente, el 9% oportuna y el 10% la calificó como nula.

El 77% de los encuestados refirió que no recibió comunicación o información del nivel regional, en relación con las estrategias definidas para la atención de los procesos sustantivos de mantenimiento y el 23% respondió que sí.

El 51% de los participantes indicó, que ha recibido información de la Dirección General y Administrativa Financiera de su centro médico, sobre las estrategias definidas para la atención de los procesos sustantivos de mantenimiento y el 49% mencionó que no.

Como se puede observar de las respuestas recibidas, a criterio de los encuestados la información y comunicación facilitada por el nivel Central y Local, no ha sido oportuna, clara y concisa; además, llama la atención que el 77% de los encuestados mencionó que el nivel regional (ARIM) no ha emitido ningún tipo de lineamiento o estrategia.

IV. SOBRE LAS ESTRATEGIAS IMPLEMENTADAS A NIVEL LOCAL PARA MITIGAR LOS EFECTOS DEL CIBERATAQUE

La gran mayoría de participantes mencionó que en sus respectivos servicios se han implementado soluciones de acuerdo con sus posibilidades, de las que resaltan las siguientes:

- Recepción de solicitudes de atención por memorándum y hojas impresas.
- Uso de recursos personales como computadora y teléfono, para coordinar con el personal y proveedores.
- Uso de máquina de escribir para la elaboración de documentación.
- Aplicación de las recomendaciones emitidas producto del oficio GIT-DMI-0448-2022.
- Impresión de formularios para solicitudes de mantenimiento.
- Registro manual de las horas hombre y materiales utilizados.
- Personal en teletrabajo siempre y cuando el perfil lo permita.
- Recorridos periódicos en los diferentes servicios del centro médico.
- Rotación de los inventarios de materiales existentes y adecuación de las obras con respecto a los materiales disponibles.
- Creación de grupos y chats de mensajería rápida (WhatsApp y Telegram).

De conformidad con lo mencionado por los participantes, se evidenció que la Administración ha implementado, de acuerdo con sus posibilidades soluciones paliativas orientadas a minimizar la afectación y garantizar la continuidad en la prestación de los servicios de salud.

V. SOBRE LOS PLANES DE CONTINGENCIA Y LA DEPENDENCIA A LOS SISTEMAS INFORMÁTICOS PARA EFECTUAR LAS LABORES SUSTANTIVAS DE MANTENIMIENTO

El 70% de los participantes mencionó que no disponían de un plan de contingencia relacionado con el ataque cibernético y el 30% opinó que sí. Así mismo, los participantes refieren una alta dependencia a los sistemas informáticos (79%) para el desarrollo de la gestión de mantenimiento, el 12% una dependencia media y el 9% una baja dependencia.

Las condiciones actuales de la tecnología nos hacen depender del uso de sistemas informáticos; no obstante, si bien es cierto los aplicativos facilitan la gestión diaria, también nos demuestra la dependencia a éstos sistemas, y el riesgo que esto conlleva, por ende, es pertinente efectuar una evaluación de los procesos, que permitan identificar, analizar y valorar los riesgos, con el objetivo de implementar actividades que minimicen los efectos que se podrían generar ante un ataque de esta naturaleza. De ahí la importancia de disponer de un plan de contingencia efectivo que mitigue las consecuencias de los eventos no deseados.

VI. SOBRE LOS FACTORES DE RIESGO IDENTIFICADOS EN EL SERVICIO DE INGENIERÍA Y MANTENIMIENTO PRODUCTO DEL ATAQUE CIBERNÉTICO

El riesgo se define como el efecto de la incertidumbre sobre los objetivos planteados, por lo cual el peor escenario sería la paralización de las labores sustantivas que se efectúa en los Servicios de Ingeniería y Mantenimiento; en ese sentido, los funcionarios participantes en el cuestionario, identificaron una serie de factores de riesgo que podrían perjudicar los procesos sustantivos que se desarrollan, como los mencionados a continuación:

- Atrasos de gestiones de caja chica, en movimientos y acciones de personal.
- Atrasos en el trámite de pago de facturas de servicios continuos.
- Incertidumbre en saldos de partidas presupuestarias.
- Procesos de sustitución de personal.
- Falta de suministros, materiales y repuestos
- Atraso de la gestión de los proyectos y pérdida de información por los equipos de cómputo infectados.
- Aumento en los tiempos de respuesta.
- Carencia de un sistema institucional alterno que contenga la información actualizada del SOCO.
- Problemas para operar equipos gestionados mediante Building Management System (BMS).
- Pocas licencias de Office 365 para el personal de mantenimiento.
- La visualización de las placas de los rayos X por el sistema EDUS, la comunicación del control de monitoreo y manejo de los aires acondicionados.
- Pérdida de información de años anteriores por el formateo de los equipos de cómputo y servidores.

En concordancia con lo anterior, el riesgo conlleva la combinación de la probabilidad de un suceso y sus efectos, en tal sentido que, en todas las organizaciones existe un potencial elevado de eventos y consecuencias que se transforman en oportunidades para conseguir beneficios o en amenazas, por lo cual, lo externado por los participantes en el cuestionario, reviste de gran importancia y refleja la realidad a la que se enfrentan actualmente los Servicios de Ingeniería y Mantenimiento.

VII. SOBRE LAS OPORTUNIDADES DE MEJORA EXTERNADAS POR LAS JEFATURAS DE LOS SERVICIOS DE INGENIERÍA Y MANTENIMIENTO

Esta Auditoría solicitó a los jefes de los Servicios de Ingeniería y Mantenimiento, referirse a las oportunidades de mejora que se podrían implementar en respuesta a la afectación sufrida producto del ciberataque, las principales observaciones se detallan a continuación:

- Disponer de sistemas de respaldo de la información en plataformas tecnológicas seguras para el resguardo de la información y el acceso remoto.
- Actualizar antivirus periódicamente.
- Disponer de un sistema informático que no dependa de la plataforma institucional y que se pueda acceder por otros medios.
- Implementar la modalidad de teletrabajo en los perfiles que se ajusten a esa medida.
- Habilitar un acceso a internet temporal para que los usuarios con Office 365 puedan tener comunicación con usuarios similares, principalmente el correo electrónico y Teams.
- Disponer de equipos portátiles.
- Mayor involucramiento del Centro de Gestión de Informática para realizar una evaluación de los riesgos y propuestas de planes de contingencia para los servicios que conforman las Unidades.
- Un acompañamiento más robusto de la DMI referente a la comunicación de lineamientos orientados a la gestión de mantenimiento.
- Implementar la modalidad de gemeleo de plazas o tiempo extraordinario para efectuar diferentes procesos entre los que se mencionan: archivo, nombramientos, atención de SOCOS, presupuesto.

- Respaldar la documentación por medio de dispositivos externos de almacenamiento, como "llave maya" o discos extraíbles.
- Efectuar actividades de coordinación entre los niveles centrales y locales, con el objetivo de generar soluciones para mejorar la gestión de ingeniería y mantenimiento.

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

> *"(…) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:*
> *a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*
> *b) Exigir confiabilidad y oportunidad de la información.*
> *c) Garantizar eficiencia y eficacia de las operaciones.*
> *d) Cumplir con el ordenamiento jurídico y técnico(...)".*

Asimismo, el artículo 16 de la Ley de marras, referente a los sistemas de información, establece:

> *"…Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados. Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.*

En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:

> *"…a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.*
> *b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficiente de los recursos públicos.*
> *c) Establecer las políticas, los procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico…".*

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

> *"…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…".*

VIII. CONSIDERACIONES FINALES

En virtud de lo anterior y con sustento en la información recopilada por esta Auditoría, resulta importante que la administración activa, valore los aspectos mencionados por los jefes de servicio de Ingeniería y Mantenimiento, relacionados con la coordinación, comunicación, claridad y suficiencia de la información, establecimiento de planes de contingencia, factibilidad de implementar el teletrabajo como una modalidad laboral en los perfiles ocupacionales que lo permitan, evaluación de los riesgos, dependencia a los sistemas informáticos; entre otros aspectos, que considera este Órgano de Control y Fiscalización se deben abordar de manera integral entre el nivel local, regional y central de la institución.

Además, en relación con la información que se está registrando manualmente en la Unidades, es importante se garantice su incorporación una vez que se restablezca el sistema (SOCO).

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 recuperación y continuidad de los servicios de Ingeniería y Mantenimiento.

Asimismo, es importante que en las acciones que se ejecuten para dar continuidad a la prestación de los servicios, se implementen los mecanismos básicos de control para garantizar la legalidad de las operaciones, igualmente, se acrediten documentalmente los lineamientos y directrices para orientar la gestión administrativa y operativa del mantenimiento, así como, la fundamentación de las decisiones que se adopten, y se mantenga la emisión de informes de rendición de cuentas a las autoridades superiores para mantenerlas al tanto de lo actuado.

Finalmente, este Órgano de Control y Fiscalización continuará efectuando las labores pertinentes dentro de nuestro ámbito de competencias, que permitan contribuir a mantener un razonable sistema institucional de control interno; además, generar valor agregado a través de las labores de asesoría y de acompañamiento en situaciones como las que enfrentamos, reconociendo que valores como la unidad, mística, responsabilidad y esfuerzo, permitirán cumplir con los objetivos planteados.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.30 12:37:17 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/ANP/MZS/PAA/SMS/ghc

C. Dr. Roberto Cervantes Barrantes, Gerente General. - 1100
Dr. Eduardo Cambronero Hernández, Director de Red de Servicios de Salud. – 2906
Auditoría